ÉCOLE DE POLITIQUE APPLIQUÉE

Faculté des lettres et sciences humaines

Université de Sherbrooke

La surveillance commerciale et sécuritaire des données personnelles : Études de cas et perspectives comparées de Google et de la National Security Agency

par

Tristan Rivard

Mémoire de maîtrise

Sherbrooke

Décembre 2017

Remerciements

Il est certain que le présent mémoire n'aurait pu aboutir sans l'implication des remercié-e-s dans mon parcours professionnel et personnel.

Tout d'abord, je remercie Pr. Karine Prémont pour sa disponibilité et sa patience en tant que directrice de recherche lors des nombreuses réorientations du sujet de mon mémoire. Ses révisions, suggestions et commentaires ont été très importantes à l'avancement et à la qualité de la rédaction. Je remercie également Pr. Hugo Loiseau, dont les précisions méthodologiques et terminologiques furent essentielles à la précision du mémoire. Les échanges et collaborations avec M. Loiseau m'ont poussé à accroître mes connaissances de la complexité technique et sociale du cyberespace, tandis que son approche appliquée m'a été d'une précieuse aide dans la vulgarisation du phénomène.

Ensuite, je remercie Alexandra Duchesne pour son écoute et son support continus durant les moments plus ardus du processus de recherche. Je remercie également Vincent Chamberland, puisque notre correspondance intellectuelle sur la cybernétique et la cyber-anthropologie m'a mené à découvrir des ouvrages, des auteurs et des concepts qui ont étoffé ma perspective sur le cyberespace.

Finalement, je veux remercier le Conseil de recherches en sciences humaines du Canada pour son financement lors de la rédaction du présent mémoire.

Table des matières

Table des acronymes

CALEA – *Communications Assistance for Law Enforcement Act*

CCTV – *Closed-Circuit Television* (télévision à circuit fermé)

CIA – *Central Intelligence Agency*

DCI – *Director of Central Intelligence*

DIA – *Defense Intelligence Agency*

EFF – *Electronic Frontier Foundation*

FAA – *FISA Amendments Act*

FISA – *Foreign Intelligence Surveillance Act*

FISC – *Foreign Intelligence Surveillance Court*

GAFAM – Google, Amazon, Facebook, Apple, Microsoft

GCHQ – *Government Communications Headquarters*

GPS – *Global Positioning System*

INR – *Bureau of Intelligence and Research*

NGA – *National Geospatial-Intelligence Agency*

NSA – *National Security Agency*

ONU – Organisation des Nations-Unies

SSO – *Special Sources Operations*

STA – *Semantic Traffic Analysis* (analyse sémantique du trafic)

TIC – Technologies de l'information et des communications

VOIP – *Voice over IP*

Introduction

L'évolution fulgurante des technologies informatiques et des moyens de communication au cours des dernières décennies annonce des changements sociopolitiques majeurs. Sur le plan de la relation de pouvoir entre les organisations étatiques et corporatives d'une part, et les individus et la société civile d'autre part, il est même possible de parler d'une transformation[1]. En effet, les nouvelles pratiques de surveillance donnent lieu à un éclatement de sa conception classique : s'ajoutent notamment depuis l'essor d'Internet la « sous-veillance[2] », faite par les citoyens envers les autorités, ainsi que la « surveillance latérale[3] », faite entre pairs dans une pluralité de contextes sociaux. Néanmoins, cet éclatement ne peut occulter le fait que ces formes de surveillance plus démocratiques ne sont pas en position de tirer profit des ressources financières, organisationnelles et techniques constitutives de l'« assemblage surveillant[4] » : l'ensemble asymétrique et décentralisé d'une multiplicité de systèmes de surveillance auparavant enclavés, mais dorénavant connectés par l'économie politique des données personnelles. Cela signifie que les agences de renseignement et les grandes corporations bénéficient d'une suprématie sur la société civile en matière d'exploitation des flux de données personnelles produits par la démocratisation des technologies de l'information et des communications (TIC).

C'est pourquoi ce projet de recherche veut décrire et analyser les dimensions sociotechniques et politiques de la surveillance des données (*dataveillance*), soit la collecte massive, continue et automatique des données produites par les usagers dans le cyberespace, telle qu'elle est conduite dans la sphère commerciale par l'entreprise Google et dans la sphère sécuritaire par la *National Security Agency* (NSA). L'objectif est d'exposer une partie des structures et des dynamiques de l'économie politique des données personnelles telle qu'elle existe aux États-Unis.

Aujourd'hui, les États-Unis sont dans une position inégalée en matière de surveillance, notamment grâce à l'importance paradigmatique de l'innovation technologique pour l'État de sécurité nationale durant la guerre froide et en raison de l'influence de celui-ci sur la création et

---

[1] Mowshowitz, Abbe, *Virtual Organization : Toward a Theory of Societal Transformation Stimulated by Information Technology*, Greenwood Publishing Group, 2002, x.
[2] Mann, Steve, Jason Nolan et Barry Wellman, « Sousveillance : Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments », *Surveillance & Society*, vol. 1, n. 3, 2003, 333.
[3] Andrejevic, Mark, « The Work of Watching One Another : Lateral Surveillance, Risk, and Governance », *Surveillance & Society*, vol. 2, n. 4, 2005, 486.
[4] Haggerty, Kevin et Richard Ericson, « The Surveillant Assemblage », *British Journal of Sociology*, vol. 51, n. 4, 2000, 605.

l'exploitation du cyberespace[5]. En effet, l'hégémonie technologique et économique de la superpuissance américaine sous-tend aussi bien le projet de la NSA de « tout collecter[6] » que la capacité de Google à indexer environ 60 trillions de pages web dans ses propres serveurs infonuagiques[7]. Dans les deux cas, la projection globale du pouvoir structurel américain[8] est manifeste : qu'il s'agisse de la prééminence de la NSA au sein des autres agences des « cinq yeux[9] » – un partenariat de surveillance réunissant l'Australie, le Canada, la Nouvelle-Zélande et le Royaume-Uni – ou bien de la présence mondiale des corporations comme Google et Facebook[10]. La surveillance des données est imbriquée au sein de relations complexes entre le quotidien des usagers, les intérêts économiques des entreprises spécialisées dans l'information et les impératifs sécuritaires des agences de renseignement. Au sein de ce triangle, les ressources principales de pouvoir sont l'accès aux banques de données[11] – le savoir numérisé – et le développement d'algorithmes de traitement des données qui soient capables de produire des informations utilisables – l'innovation technologique.

Dans le premier chapitre, nous contextualiserons l'économie politique des données personnelles et les fonctions que sert la surveillance des données. Nous survolerons ensuite la littérature des « études sur la surveillance » de sorte à présenter certains concepts clés, dont celui de « nébuleuse de surveillance étatique-corporative ». Nous préciserons ensuite le cadre opérationnel et méthodologique de notre recherche. Aux chapitres deux et trois, nous procéderons à une étude de cas de Google et de la NSA décrivant les contextes, les cibles, les principes, les tactiques et les stratégies de surveillance des deux organisations. Dans le dernier chapitre, nous comparerons les deux études de cas et les rôles commerciaux et sécuritaires de la

---

[5] Hargittai, Eszter, *Holes in the Net : The Internet and International Stratification*, 1996, URL : http://www.isoc.org/inet98/proceedings/5d/5d_1.htm (consulté le 4 décembre 2017).
[6] Nakashima, Ellen et Joby Warrick, « For NSA chief, terrorist threat drives passion to 'collect it all' », *The Washington Post*, 14 juillet 2013, URL : https://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html (consulté le 4 décembre 2017).
[7] Google, « How Search Works », *Google Inside Search*, 2016, URL : http://www.google.com/insidesearch/howsearchworks/thestory/ (consulté le 4 décembre 2017).
[8] Cerny, Philip, « Dilemmas of Operationalizing Hegemony », chapitre dans Mark Haugaard et Howard Lentner, *Hegemony and Power : Consensus and Coercion in Contemporary Politics*, Lexington Books, 2006, 83.
[9] Farrell, Paul. « History of 5-Eyes – explainer », *The Guardian*, 2 décembre 2013, URL : http://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer (consulté le 4 décembre 2017).
[10] Narayana, Nagesh, « Google, Facebook and Youtube outshine others in web globalization », *International Business Times*, 2011, URL : http://www.ibtimes.com/google-facebook-youtube-outshine-others-web-globalization-278813 (consulté le 4 décembre 2017).
[11] Lyotard, Jean-François, *The Postmodern Condition : A Report on Knowledge*, University of Minnesota Press, 1984, 14.

surveillance de masse des données personnelles. La conclusion porte vers deux constats : d'abord, que les deux formes de surveillance sont complémentaires au niveau de la sécurisation du cyberespace, même si elles opèrent selon des incitatifs et des fins explicitement distinctes ; ensuite, que l'implication des surveillés dans la reproduction des pratiques et des structures qui opérationnalisent la surveillance remet en question la validité analytique des conceptions binaires dans le cyberespace, notamment celles fondées sur une opposition entre la liberté et le contrôle ainsi qu'entre l'autonomie et le conditionnement.

Chapitre 1: Cadre théorique et méthodologique

Ce premier chapitre explicite le cadre théorique et le cadre méthodologique de la recherche.

1.1. Cadre théorique

Le cadre théorique de la recherche aborde la problématique de la transformation du fonctionnement, des principes et du rôle de la surveillance au 21e siècle ; il pose également les questions qui orientent notre réflexion et les notions importantes présentes dans la littérature.

1.1.1. Problématique

Évidemment, tous les États modernes pratiquent une forme plus ou moins développée de surveillance à l'intérieur et à l'extérieur de leur territoire. Néanmoins, le processus de numérisation génère de nouvelles dynamiques qui se distinguent de celles associées à la surveillance basée sur l'encre et le papier. Les documents physiques imposent des limites structurelles sur les possibilités et processus de surveillance, ne serait-ce qu'en vertu de la complexité de leur accumulation, de leur croisement et de leur recherche[12]. Ces limites inhérentes au médium du papier favorisent une surveillance sélective, à la fois dans son intensité sur une seule cible et dans sa portée sur plusieurs cibles. Or, les technologies de l'information abrogent ces limitations matérielles en permettant une surveillance instantanée, invisible, automatisée, permanente et continue de l'information. De plus, la connexion en réseau de différents systèmes de surveillance auparavant enclavés accroît la profondeur et la portée de l'information accessible aux organisations :

> Pour la première fois dans l'histoire, les gouvernements et les corporations ont la capacité de conduire une surveillance de masse sur des populations entières. Ils peuvent le faire avec notre utilisation d'Internet, nos communications, nos transactions financières, nos mouvements… Même les Allemands de l'Est ne pouvaient suivre tout le monde tout le temps. […] Ceci est la surveillance de masse, impossible sans les ordinateurs, les réseaux et l'automatisation[13].

Ce précédent historique occasionné par les technologies numériques et réticulaires transforme certes les techniques de surveillance, mais il implique aussi une généralisation socioculturelle et populaire des principes de la surveillance, notamment par l'entremise des médias sociaux. En définitive, la généralisation du phénomène introduit les entreprises et les usagers au sein de pratiques jadis réservées aux hautes sphères de l'État.

---

[12] Ellul, Jacques. *The Technological Society*, Vintage Books, 1964, 249.

[13] Cette citation et les suivantes sont des traductions libres de l'auteur. Schneier, Bruce, *Data & Goliath – The Hidden Battles to Collect Your Data and Control Your World*, W. W. Norton & Company, 2015, 27-28.

Des changements qualitatifs, il est admis que l'accessibilité des technologies de l'information permet une démocratisation des possibilités de surveillance[14], altérant du coup la nature essentiellement élitiste et hiérarchique de la surveillance bureaucratique[15]. Conjuguées, la généralisation et l'intensification des pratiques rendent la surveillance « rhizomique », un terme emprunté à la botanique par Gilles Deleuze et Felix Guattari pour représenter une multiplicité hétérogène, décentralisée et interconnectée, qui croît de façon non-linéaire[16]. En ce sens, la surveillance connaîtrait actuellement une prolifération massive, mais non coordonnée, sous l'impulsion de multiples intérêts gouvernementaux, commerciaux et populaires : « les technologies surveillantes opèrent par variation et disjonction, intensification et expansion horizontale fragmentaire[17] ». En somme, la surveillance du 21e siècle est complexe : plutôt que de s'ériger en figure monolithique et centralisée, elle est caractérisée par une multiplicité de regards entrecroisés qui scrutent différents éléments d'un vaste réseau d'information personnelle[18]. Elle donne lieu à un foisonnement de stratégies sociotechniques exploitant l'« infinité de combinaisons dans l'utilisation de ces ressources : contrôle, savoir, sociabilité, gestion d'identité personnelle, diverses formes de surveillance, de résistances politiques, de profit, etc.[19] ».

En ce qui concerne les changements quantitatifs, il est commun de citer le fait que les processeurs informatiques connaissent une croissance « exponentielle[20] », leur puissance de traitement étant plus ou moins doublée tous les 18 mois depuis des décennies, en accord avec la « loi de Moore[21] » – bien que celle-ci soit l'objet de maintes critiques insistant sur d'importantes limites conceptuelles et empiriques[22]. Ces capacités de traitement croissantes sous-tendent les pratiques analytiques fondées sur les mégadonnées (*big data*) : l'utilisation de logiciels

[14] Goldsmith, A. J., « Policing new visibility », *British Journal of Criminology*, vol. 50, n. 5, 914.
[15] Arora, Rahul, « Encyclopaedic Dictionary of Organization Behaviour », vol. 2, Sarup & Sons, 2000, 337.
[16] Deleuze, Gilles et Felix Guattari, *A Thousand Plateaus*, University of Minnesota Press, 1987, 6, 10.
[17] Hier, Sean, « Probing the Surveillant Assemblage : on the dialectics of surveillance practices as processes of social control », *Surveillance & Society*, vol. 1, n. 3, 2003, 403.
[18] Haggerty, Kevin et Richard Ericson, « The Surveillant Assemblage », 618.
[19] Zavala Pérez, Maria, « Registry Culture and Networked Sociability : Building Individual Identity through Information Records », chapitre dans Francesca Comunello, *Networked Sociability and Individualism : Technology for Personal and Professional Relationships*, IGI Global, 2011, 50.
[20] Sneed, Annie, « Moore's Law Keeps Going, Defying Expectations », *Scientific American*, 2015, URL http://www.scientificamerican.com/article/moore-s-law-keeps-going-defying-expectations/ (consulté le 4 décembre 2017).
[21] Encyclopaedia Britannica, « Moore's law », *Encyclopedia Britannica*, s/d, URL : www.britannica.com/topic/Moores-law (consulté le 4 décembre 2017).
[22] Ganasca, Jean-Gabriel, *Le mythe de la singularité*, Éditions du Seuil, 2017, 33.

sophistiqués pour croiser plusieurs bases de données massives en vue de révéler des tendances et des relations utiles à une organisation[23]. Les mégadonnées sont de plus en plus perçues comme panacée décisionnelle par les gouvernements et les industries pouvant bénéficier d'une réduction des risques, notamment par l'analyse prédictive[24]. L'utilité générale de ces pratiques analytiques aux domaines de la santé, de la sécurité nationale, des sciences humaines, de la finance, du marketing et de la gestion administrative en général[25] est un incitatif majeur à la collecte d'information personnelle, qui sous-tend la construction de vastes centres de données consommant collectivement 1,5% de l'électricité mondiale[26].

De ces transformations qualitatives et quantitatives de la surveillance émerge une économie politique des données personnelles[27], uniquement concevable dans un environnement sociotechnique où les populations produisent, communiquent et cèdent leurs informations à des organisations par l'entremise des technologies informatiques[28]. La surveillance traditionnelle faisait porter au surveillant la responsabilité de générer des informations; or, la surveillance informatique procède, en majeure partie, des données produites et communiquées par les surveillés eux-mêmes[29]. Ce renversement des rôles n'est pas étranger à l'immatérialité du cyberespace : si la surveillance traditionnelle était intrinsèquement limitée par sa visibilité et sa physicalité (par exemple, un surveillant ou un artefact matériel étant requis), la surveillance informatique bénéficie de l'ubiquité et de l'invisibilité du cyberespace[30].

En effet, les logiciels, services et site web du cyberespace sont structurés par des politiques

---

[23] Curry, Edward, « The Big Data Value Chain : Definitions, Concepts, and Theoretical Approaches », chapitre dans José Maria Cavanillas, Edward Curry et Wolfgang Wahlster, *New Horizons for a Data-Driven Economy*, Springer Open, 2016, 30.
[24] Kerschberg, Ben, « Five Steps to Master Big Data and Predictive Analytics in 2014 », *Forbes*, 2014, URL : www.forbes.com/sites/benkerschberg/2014/01/03/five-steps-to-master-big-data-and-predictive-analytics-in-2014/#2f018a816f43 (consulté le 4 décembre 2017).
[25] Curry, Edward, « The Big Data Value Chain : Definitions, Concepts, and Theoretical Approaches », 34-35.
[26] Levy, Steven, « Google Throws Open Doors to Its Top-Secret Data Center », *Wired*, 17 octobre 2012, URL http://www.wired.com/2012/10/ff-inside-google-data-center/ (consulté le 4 décembre 2017).
[27] Gandy, H. Oscar, « The Political Economy of Personal Information », chapitre dans Janet Wasko, Graham Murdock et Helena Sousa, *The Handbook of Political Economy of Communications*, Blackwell Publishing, 2011, 436.
[28] Anthony Maurno, Dann et Louis Sirico, *Thin Air : How Wireless Technology Supports Lean Initiatives*, CRC Press, 2010, 106.
[29] Fuchs, Christian, « The Political Economy of Privacy on Facebook », *Television New Media*, vol. 13, n. 2, 151-152.
[30] Gilliom, John, « Struggling with Surveillance : Resistance, Consciousness, and Identity », chapitre dans Richard Victor Ericson et Kevin Haggerty, *The New Politics of Surveillance and Visibility*, University of Toronto Press, 2006, 121.

souvent invisibles[31], qu'il s'agisse d'une interface particulière ou encore des logiques d'un algorithme de collecte de données[32], de croisement des bases de données (*data matching*) ou d'extraction de connaissances à partir des données (*data mining*)[33]. Considérant que la vie politique est infléchie par la structure des systèmes communicationnels[34], il est indéniable que la prégnance du cyberespace génère des changements politiques d'importance[35].

La transformation de la surveillance est accélérée par l'intégration rapide du cyberespace à la vie quotidienne, particulièrement avec la popularisation des médias sociaux et des plateformes d'échange de contenu produit par les utilisateurs. Cet engouement populaire est constatable tous les jours, mais s'illustre sans équivoque dans les statistiques suivantes : plus de 30 milliards de pièces d'information sont partagées tous les mois sur le média social Facebook ; plus de 35 heures de vidéo sont mises en ligne toutes les minutes sur la plateforme YouTube[36]. Cette effervescence populaire contraste avec les propensions monopolistiques de l'économie politique numérique, qui donnent lieu à de « grands empires postindustriels[37] » comme Google. La dynamique de « gagnant emporte tout » qui prévaut dans le cyberespace est alimentée par la structure centripète de l'effet de réseau[38]. C'est notamment le cas de Google et de Facebook, dont la concentration d'une masse critique d'utilisateurs génère un cercle vertueux de production de données qui en font des acteurs prédominants du cyberespace[39]. Donc, si le médium numérique démocratise l'accès à l'information, il contribue néanmoins, par le coût marginal presque nul des opérations et de l'information, à diverses formes de monopole et de

[31] Murakami Wood, David, « Vanishing Surveillance : Why Seeing What is Watching Us Matters », *Office of the Privacy Commissioner of Canada*, 2011, URL : www.priv.gc.ca/information/research-recherche/2011/wood_201107_e.asp (consulté le 4 décembre 2017).
[32] Gillespie, Tarleton, « The Relevance of Algorithms », chapitre dans Tarleton Gillespie, Pablo Boczkowski et Kirsten Foot, *Media Technologies – Essays on Communication, Materiality, and Society*, MIT Press, 2014, 168-169.
[33] Australian Law Reform Commission, « 9. Overview : Impact of Developing Technology on Privacy », *ALRC Report 108*, 2008, URL : www.alrc.gov.au/publications/9.%20Overview%3A%20Impact%20of%20Developing%20Technology%20on%20Privacy/data-matching-and-data-mining (consulté le 4 décembre 2017).
[34] O'Neill, John, « Bio-Technology : Empire, Communications and Bio-Power », *Canadian Journal of Political and Social Theory*, vol. 10, n. 1-2, 1986, 66.
[35] Crampton, W. Jeremy, *The Political Mapping of Cyberspace*, University of Chicago Press, 2003, 1.
[36] Maria Zavala Pérez, « Registry Culture and Networked Sociability : Building Individual Identity through Information Records », 50.
[37] Cueva, Mateo, « Cyber-Léviathan », *Société de l'information et coopération internationale*, vol. 22, n. 2, 2003, 228.
[38] Tillinac, Jean, « Le web 2.0 ou l'avènement du client ouvrier », *Quaderni*, vol. 60, n. 1, 2006, 20.
[39] Tillinac, Jean, « Le web 2.0 ou l'avènement du client ouvrier ».

centralisation informationnelle[40].

Visiblement, l'exploitation commerciale des données personnelles est une facette importante de la surveillance informatique[41]. La dimension sécuritaire avait été peu soulevée dans les médias avant que les fuites du lanceur d'alerte Edward Snowden révèlent l'existence d'un vaste système de surveillance développé par la NSA, avec la coopération des pays anglo-saxons membres des « cinq yeux ». Cette infrastructure globale destinée à « collecter tous les signaux [électroniques], tout le temps[42] », implique une mobilisation totale et constante des nouvelles technologies au nom de la sécurité nationale : télévision en circuit fermé (CCTV), médias sociaux, données cellulaires, serveurs des grandes corporations du web, l'« Internet des choses », intelligences artificielles, mégadonnées, etc.[43].

Si la surveillance commerciale est souvent considérée bénigne[44], le potentiel d'abus par la surveillance sécuritaire est plus manifeste, notamment en matière de droit à la vie privée et à la libre expression ainsi que de la viabilité du cyberespace lui-même[45]. L'intégration du cyberespace à la logique sécuritaire constitue une problématique globale en vertu de la propension du médium informatique à fusionner les réseaux de communication pour les reconstituer sur le modèle d'un « village planétaire[46] », transformant significativement la conception et le potentiel traditionnels des communications. En effet, l'ubiquité des réseaux informatiques dans les structures administratives et la vie quotidienne des populations civiles d'Occident érode la séparation entre la vie publique et privée[47] et entre les structures étatiques et

[40] The Economist, « Should digital monopolies be broken up ? », *The Economist*, 29 novembre 2014, URL : http://www.economist.com/news/leaders/21635000-european-moves-against-google-are-about-protecting-companies-not-consumers-should-digital (consulté le 4 décembre 2017).
[41] McStay, Andrew, *Digital Advertising*, Palgrave Macmillan, 2009, 89.
[42] Selon les propos du directeur de la NSA de 2005 à 2014, Keith Alexander. Kopstein, Joshua, « The NSA Can 'Collect-it-All', But What Will It Do With Our Data Next? », *The Daily Beast*, 16 mai 2014, URL : http://www.thedailybeast.com/articles/2014/05/16/the-nsa-can-collect-it-all-but-what-will-it-do-with-our-data-next.html (consulté le 4 décembre 2017).
[43] Lyon, David, « Surveillance, Snowden, and Big Data : Capacities, consequences, critique », *Big Data & Society*, juillet 2014, 2.
[44] Lyon, David, « The Politics of Surveillance », chapitre dans *Surveillance Society : Monitoring Everyday Life*, McGraw-Hill Education, 2001, 127.
[45] Deibert, Ronald, « Black Code : Censorship, Surveillance, and the Militarisation of Cyberspace », *Millenium – Journal of International Studies*, vol. 32, n. 3, 502.
[46] McLuhan, Marshall et Quentin Fiore, *The Medium is the Massage*, Gingko Pr Inc, 2001, 63.
[47] Crampton, Jeremy, *The Political Mapping of Cyberspace*, 138.

corporatives[48], en plus de précariser le « droit d'être laissé à soi-même[49] ». L'appropriation de l'espace numérique par les structures de pouvoir étatiques et corporatives est donc une situation ayant des conséquences sociétales élargies par la nature intégrative et ubiquitaire[50] du médium.

Le cyberespace est l'objet d'une réappropriation par trois discours hégémoniques : militairement, par la « révolution dans les affaires militaires[51] » ; économiquement, par la consécration du capitalisme postfordien avec le développement du commerce en ligne[52] ; culturellement, en tant qu'espace civilisationnel diffusant surtout des valeurs occidentales, voire américaines[53]. De ce fait, dans la mesure où les « perturbations numériques[54] » se font sentir, c'est davantage en tant que « destruction créatrice[55] » ouvrant la voie à de nouvelles opportunités politiques et économiques pour les puissances dominantes[56] qu'en tant que subversion des structures de pouvoir. En fait, ces dernières se prolongent au sein du nouveau champ d'action et de communication[57] :

> La technologie de computation et l'Internet n'ont pas été inventés dans des contextes économiques, mais militaires, et face à la Seconde Guerre mondiale (l'ordinateur) et la guerre froide (Internet). Mais la diffusion sociétale de ces technologies est due au rôle qu'elles ont joué primairement pour la restructuration économique du capitalisme. […] Les réseaux d'ordinateurs sont la fondation technologique ayant permis l'émergence d'un réseau global du capitalisme : soit, des régimes d'accumulation, de régulation et de discipline qui aident à baser l'accumulation du capital économique, politique et culturel de plus en plus sur des organisations transnationales en réseau qui

[48] Garrie, Daniel, « The Need for Private-Public Partnerships Against Cyber Threats – Why A Good Offense May Be Our Best Defense », *Huffinton Post*, 4 janvier 2016, URL : www.huffingtonpost.com/daniel-garrie/the-soft-power-war-isis-d_b_8818866.html (consulté le 4 décembre 2017).
[49] The Economist. *The Right to be left alone*, 19 janvier 2015, URL : www.economist.com/news/science-and-technology/21639988-why-do-people-cherish-privacy-yet-cheerfully-surrender-it-right-be-left-alone (consulté le 4 décembre 2017).
[50] Hurley, Matthew, « For and From Cyberspace – Conceptualizing Cyber Intelligence, Surveillance, and Reconaissance », *Air & Space Power Journal*, novembre-décembre 2012, 18.
[51] Keohane, O. Robert et Joseph S. Nye, « Power and interdependence in the information age », *Foreign Affairs*, vol. 77, n. 5, septembre-octobre 1998, 88.
[52] Agger, Ben, *Postponing the Postmodern : Sociological Practices, Selves, and Theories*, Rowman & Littlefield, 2002, 112.
[53] Nye, S. Joseph, « The Information Revolution and American Soft Power », *Asia-Pacific Review*, vol. 9, n. 1, 2002, 60.
[54] Schmidt, Eric et Jared Cohen, « The Digital Disruption : Connectivity and the Diffusion of Power », *Foreign Affairs*, vol. 89, n. 6, 2010, 75, URL : https://www.foreignaffairs.com/articles/2010-10-16/digital-disruption (consulté le 4 décembre 2017).
[55] Schumpeter, A. Joseph, *Capitalism, Socialism and Democracy*, Harper, 1942, 82.
[56] MacGregor, D. et al., « Convergence Platforms : Human-Scale Convergence and the Quality of Life », chapitre dans Milhail Roco et al., *Convergence of Knowledge, Technology and Society : Beyond Convergence of Nano-Bio-Info-Cognitive Technologies*, Springer Science & Business Media, 2014, 71.
[57] McEvoy Manjikian, Mary, « From Global Village to Virtual Battlespace; The Colonizing of the Internet and the Extension of Realpolitik », *International Studies Quarterly*, vol. 54, n. 2, 2010, 385.

> font usage du cyberespace […] pour une coordination et une communication globales[58].

En ôtant de nombreuses limites techniques relatives à l'organisation et à l'articulation du pouvoir, les TIC et le cyberespace donnent lieu à une redéfinition du contrat social[59]. La dualité entre les libertés fondamentales relativement statiques – qui ont pour fonction de freiner l'arbitraire du pouvoir – et la croissance effervescente du savoir et du pouvoir technique – qui tend vers l'efficience systémique – soulève une question centrale à la pérennité des sociétés industrielles avancées : est-ce que la concomitance historique du libéralisme et de la dynamique technoscientifique aux 18e et 19e siècles dissimule leur état de tension latent et croissant à mesure que le monde sociopolitique est technicisé[60]? Plus spécifiquement, l'orientation de la productivité humaine vers le projet technoscientifique et ses impératifs systémiques peut-elle aller à l'encontre des fondements humanistes et individuels du libéralisme[61] ? Ces questions sont d'autant plus pertinentes qu'il est généralement admis que le cadre libéral et démocratique des sociétés industrielles avancées soit un facteur contraignant les structures techno-économiques. Pourtant, les décisions prises en matière de développement technologique échappent aux délibérations démocratiques et opèrent directement sur les conditions sociotechniques qui déterminent les conditions de vie des populations. Certaines réalités, dont l'État de sécurité nationale et les révélations sur la surveillance informatique de masse, indiquent une préséance de l'exploitation politique des technologies – selon l'impératif épistémique de la sécurité nationale – sur les limitations juridiques et éthiques des régimes libéraux[62].

En observant la problématique de la surveillance à l'ère de la « révolution globale de l'information[63] », nous avons pu constater que cette dernière génère des effets objectifs, sur les arrangements matériels des communications et des structures de pouvoir, et intersubjectifs, dans

---

[58] Fuchs, Christian. *Internet and Society : Social Theory in the Information Age*, Routledge, 2008, 87.
[59] Joseph Skovira, Robert, « The Social Contract Revised : Obligation and Responsibility in the Information Society », chapitre dans Hamid Nemati, *Information Security and Ethics : Concepts, Methodologies, Tools, and Applications*, IGI Global, 2007, 2804.
[60] Guston, David, « The essential tension in science and democracy », *Social Epistemology : A Journal of Knowledge, Culture and Policy*, vol. 7, n. 1, 1993, 3.
[61] Agazzi, Evandro, « From Technique to Technology : The Role of Modern Science », *Philosophy & Technology*, vol. 2, n. 4, hiver 1998, 9.
[62] Magalhaes, Roy, *Organizational Knowledge and Technology : An Action-Oriented Perspective on Organization and Information Systems*, Edward Elgar Publishing, 2004, 166.
[63] Price, E. Monroe, *Media and Sovereignty – The Global Information Revolution and Its Challenge to State Power*, The MIT Press, 2002, 1.

les comportements et attitudes individuelles relatives au nouvel environnement sociotechnique. Il semble alors nécessaire que l'étude des pratiques de surveillance procède d'une contextualisation soucieuse des tendances contemporaines de l'économie politique et attentive à la récente constitution de structures étatiques et corporatives destinées à la « domination technologique globale[64] ».

1.1.2. Question générale de recherche

Le survol de la problématique illustre la complexité des interrelations dans le cyberespace entre les populations d'usagers et les structures de pouvoir de l'économie politique des données numériques, ce qui donne lieu à plusieurs questionnements. L'intégration et l'ubiquité du cyberespace fait converger les mondes médiatiques, politiques, économiques, culturels et sociaux, tout en rendant ce processus difficilement perceptible[65]. Cette convergence soulève de nombreuses questions dans la littérature scientifique sur l'économie politique de la surveillance et du cyberespace. Que signifie une telle transformation pour la relation entre les citoyens, le secteur privé et l'État? Est-ce que le médium informatique donne lieu à une forme d'économie politique inédite ou ne fait-il que modifier celle existante? En quoi le cyberespace altère-t-il l'asymétrie de savoir et de pouvoir entre les individus et les organisations politico-économiques? Finalement : quelles formes de surveillance sont favorisées par l'économie politique des données numériques? À bien des égards, la littérature développée par les « études sur la surveillance[66] » offre des réponses à ces questions, selon une approche critique attentive à l'évolution des configurations de pouvoir dans le cyberespace. En ce qui concerne notre question générale de recherche, il est question de comprendre quels acteurs, quels processus et quelles dynamiques sous-tendent l'exploitation des données des usagers du cyberespace.

1.1.3. Revue de la littérature

La revue de la littérature procède à l'économie conceptuelle des champs académiques foisonnant que sont les études de la surveillance et les contributions critiques à l'économie politique. Elle se concentre sur les notions d'une adaptation des organisations et structures capitalistes aux technologies informationnelles, d'une convergence des intérêts public et privés au sein d'une

[64] Purkayastha, P., « New Technologies and Emerging Structures of Global Dominance », *Economic and Political Weekly*, vol. 29, n. 35, 1994, 102.
[65] McLuhan, Marshall et Quentin Fiore, *The Medium is the Massage*, 16, 63.
[66] Surveillance Studies Centre, *About*, 2016, URL : www.sscqueens.org/about (consulté le 4 décembre 2017).

« nébuleuse de surveillance étatique-corporative » ainsi que d'une logique liant la sécurité des systèmes à l'autonomie individuelle, la gouvernementalité.

1.1.3.1. Capitalisme informationnel et économie politique des données numériques

Les champs académiques respectifs aux études de surveillance et à l'économie politique des données définissent les postulats et concepts fondamentaux pour réfléchir aux relations entre la surveillance et les tendances plus larges de l'économie politique internationale. En effet, ces disciplines décloisonnent les diverses formes de surveillance du contexte strictement sécuritaire afin d'analyser leur diffusion parmi les phénomènes économiques, culturels et politiques contemporains[67].

D'emblée, le point de départ de nombreuses contributions à la littérature est l'ensemble des changements sociétaux occasionnés par le développement d'une « société de l'information » et des ensembles sociotechniques qui la sous-tendent.

> L'attention centrale de l'activité économique dans les sociétés post-industrielles se déplace de la production d'objets à la gestion d'information et de savoir. Le pouvoir des grandes firmes transnationales repose maintenant autant sur leurs capacités à organiser l'information et le savoir que sur leur rôle traditionnel dans des activités directement productives[68].

Le développement d'une industrie destinée à l'exploitation et à la marchandisation des données personnelles des usagers s'inscrit dans cette dynamique plus large de réorientation informationnelle du capitalisme : « En conséquence, les ''industries du savoir'' – éducation, traitement de l'information, recherche et développement – sont devenues les secteurs les plus importants des sociétés industrielles avancées[69] ». Cette tendance économique est propice à la diffusion socioculturelle des principes et pratiques de la surveillance, particulièrement dans un contexte de globalisation et démocratisation des technologies de l'information et des communications. En effet, d'après le chercheur Bruce Schneier, les géants d'Internet comme Google et Facebook, qui offrent des services en apparence gratuits à plus d'un milliard d'usagers, sont d'importants vecteurs de la réduction de l'anonymat en ligne par le biais de leurs pratiques publicitaires ciblées individuellement. Selon l'auteur, la surveillance constituerait en

[67] Verde Garrido, Miguelangel, « Contesting a Biopolitics of Information and Communication », *Surveillance & Society*, vol. 13, n. 2, 2015, 155.
[68] Cruise O'Brien, Rita et G. K. Helleiner, « The Political Economy of Information in a Changing International Economic Order », *International Organization*, vol. 34, n. 4, 1980, 445.
[69] Gilpin, Robert, *US Power and the Multinational Corporation*, Basic Books, 1975, 166.

fait « le modèle d'affaires de l'Internet[70] ».

De plus, la relation entre les intérêts capitalistes et la généralisation des pratiques de surveillance souligne le rôle pivot joué par certaines corporations en tant qu'intermédiaires entre les masses d'usagers et les agences de renseignement. En effet, le support volontaire et involontaire des corporations associées à la *Silicon Valley* et aux télécommunications est essentiel au déploiement des programmes de surveillance planétaire conduits par la NSA[71]. Par exemple, la concentration croissante du marché des télécommunications, stimulée par sa dérégulation en 1996[72], facilite la coopération entre les agences de renseignement américaines et les multinationales essentielles à la portée globale de la surveillance, dont AT&T[73]. Il y a alors lieu de parler d'une extension informelle des stratégies politiques du gouvernement étasunien à travers certaines grandes corporations, ce qui cadre avec la notion d'une diffusion de la puissance structurelle avec la globalisation néolibérale[74] :

> [La] surveillance est devenue globalisée simplement parce que les processus économiques et politiques sont eux-mêmes globalisés, pour le meilleur ou pour le pire. […] La globalisation de la surveillance, comme toutes les autres globalisations, est à la fois un phénomène à part entière et quelque chose qui a lieu de différentes façons dans différents pays, produisant des situations d'interrelations complexes. Dans certains cas, la surveillance est « glocalisée » étant donné que les circonstances locales font une réelle différence sur les tendances générales[75].

Cet aspect « glocal » est particulièrement approprié au contexte américain, puisque les pratiques de surveillance de ses grandes entités publiques et privées reflètent la position incontestée du pays en matière de développement technomilitaire[76]. En tant que superpuissance militaire et première puissance économique, les États-Unis jouissent d'un capital technique, financier et

---

[70] Schneier, Bruce, « 'Stalker Economy' here to stay », *CNN*, 26 novembre 2013, URL : http://edition.cnn.com/2013/11/20/opinion/schneier-stalker-economy/index.html (consulté le 4 décembre 2017).
[71] Verde Garrido, Miguelangel, « Contesting a Biopolitics of Information and Communication », 154.
[72] Noam, Eli, *The Effect of Deregulation on Market Concentration : an Analysis of the Telecom Act of 1996 and the Industry Meltdown*, 2002, URL : www.citi.columbia.edu/elinoam/articles/Effect_of_Deregulation_on_MarketConcentration.pdf (consulté le 4 décembre 2017).
[73] Angwin, Julia, Charlie Savage *et al*., « AT&T Helped U.S. Spy on Internet on a Vast Scale », *The Guardian*, 15 août 2015, URL: http://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html?_r=0 (consulté le 4 décembre 2017).
[74] Carroll, William et Colin Carson, « Neoliberalism, capitalist class formation and the global network of corporations and policy groups », chapitre dans Dieter Plehwe, Bernhard Walper et Gisela Neunhöffer, *Neoliberal Hegemony : A Global Critique*, Routledge, 2007, 67.
[75] Lyon, David, *Surveillance Studies : An Overview*, Polity Press, 2007, 134-135.
[76] Engelhardt, Tom. *Shadow Government – Surveillance, Secret Wars, and a Global Security State in a Single-Superpower World*, Haymarket Books, 2014, 114.

organisationnel inégalé[77]. La surveillance commercialisée contribue alors au projet politico-militaire de « domination informationnelle », définie comme le « degré de domination dans le domaine de l'information qui permette la conduite d'opérations sans opposition effective[78] ». Ce capital se constate autant dans les investissements massifs vers le département de la Défense – dont les activités requièrent de manière croissante l'emploi de hautes technologies[79] –que dans la masse critique d'usagers des « quatre grands » acteurs d'Internet, tous basés aux États-Unis (Google, Amazon, Facebook, Apple)[80]. Les manifestations concrètes de la surveillance informatique sont donc indissociables du primat techno-militaire américain.

1.1.3.2. La « nébuleuse de surveillance étatique-corporative » comme axiome de globalisation de la surveillance

Dans une contribution majeure au champ des études sur la surveillance, les auteures Kirstie Ball et Laureen Snider soutiennent que la société de surveillance globalisée favorise les intérêts des « deux configurations massives du pouvoir[81] », c'est-à-dire les États et les corporations multinationales : ces deux entités sont les mieux adaptées pour tirer profit d'une collecte et d'un traitement de grandes masses de données personnelles. La littérature souligne que l'État et les grandes entreprises seraient de plus en plus interdépendants en matière de surveillance informatique, au point de désigner la convergence vers des méthodes et des logiques similaires au moyen du concept de « nébuleuse de surveillance étatique-corporative » (*state-corporate nexus*)[82]. Cette interdépendance se manifeste notamment dans les technologies à double usage, qui sont originellement développées pour l'État à des fins militaires et subséquemment adaptées et commercialisées à des fins de consommation, comme le *Global Positioning System* (GPS) et l'Internet[83]. Selon Zygmunt Bauman, la relation État-corporation relative à l'économie politique

[77] Piero Siroli, Gian, « Strategic Information Warfare : An Introduction », chapitre dans Martin Bayer, *Cyberwar, Netwar and the Revolution in Military Affairs*, Palgrave MacMillan, 2006, 32-33.
[78] Ralston, Joseph et Paul Kaminiski, « Chapter IV – Achieving Joint Warfighting Capability Objectives : Information Superiority », *Joint Warfighter S&T Plan*, 1997, URL : http://fas.org/spp/military/docops/defense/97_jwstp/jw4a.htm (consulté le 4 décembre 2017).
[79] Piero Siroli, Gian, « Strategic Information Warfare : An Introduction », 33.
[80] Boulanger, Philippe, *Géopolitique des médias : Acteurs, Rivalités et Conflits*, Armand Colin, 2014, 155.
[81] Ball, Kirstie et Laureen Snider, *The Surveillance-Industrial Complex : A Political Economy of Surveillance*, Routledge, 2013, 1-2.
[82] Ball, Kirstie et David Murakami Wood, « Editorial : Political Economies of Surveillance », *Surveillance & Society*, n. 1-2, vol. 11, 3.
[83] Knight, Judson, « Dual Use Technology », dans K. Lee Lerner et Brenda Lerner, *Encyclopedia of Espionage, Intelligence, and Security*, Gale, 2004, 364.

de la surveillance serait définie par la concomitance d'au moins trois processus : la numérisation, la privatisation et la transnationalisation[84]. Leur approfondissement facilite selon l'auteur « l'intégration des processus de surveillance au sein des activités et agendas du capital global et de l'État[85] ».

La nébuleuse de surveillance étatique-corporative implique une relation itérative composée d'actions et de réactions entre les deux structures de pouvoir. D'un côté, les multinationales ont « financé, conçu, légitimé et construit les appareils de la surveillance[86] », comme les téléphones cellulaires et les ordinateurs personnels, dont la structure de fonctionnement impose divers processus de collecte et de rétention de données. Les entreprises sont les principales instigatrices du processus de « mise en données[87] » (*datafication*), soit la conversion des actions et activités des usagers en données standardisées et quantifiées, y voyant une manne commerciale à exploiter. Sur une échelle de masse, la mise en données des activités et des communications humaines constitue un précédent en matière de « lisibilité des populations[88] » par les structures de pouvoir, puisqu'il permet une surveillance automatisée, un suivi à distance en temps réel, la visualisation des relations sociales et l'analyse prédictive par algorithme[89]. De l'autre côté, les États – en particulier les États-Unis – s'adaptent aux risques posés par la généralisation des communications informatiques et la structure globale d'Internet par « une transformation plus large affectant la façon dont les limites de la sécurité nationale fonctionnent[90] ». Les États-Unis mènent la constitution d'une « technopolitique[91] » cherchant à intégrer politiquement les innovations technologiques de sorte que l'État de sécurité nationale demeure en amont des changements sociaux, économiques et culturels que ces innovations génèrent. Plus précisément, la relativisation des frontières dans le cyberespace serait appréhendée par le département de la

[84] Bauman, Zygmunt *et al*., « After Snowden : Rethinking the Impact of Surveillance », 126.
[85] Ball, Kirstie et Laureen Snider. *The Surveillance-Industrial Complex,* 5.
[86] Ball, Kirstie et Laureen Snider. *The Surveillance-Industrial Complex*, 3-4.
[87] Mayer-Schoenberger, V. et K. Cukier, *Big Data – A Revolution that will transform how we live, work, and think*, John Murray Publishers, 2013, 30.
[88] Scott, C. James, *Seeing Like A State : How Certain Schemes to Improve the Human Condition Have Failed*, Yale University Press, 1999, 183.
[89] Van Dijck, José, « Datafication, Dataism and Dataveillance : Big Data between scientific paradigm and ideology », *Surveillance & Society*, vol. 2, n. 12, 2014, 198.
[90] Bauman, Zygmunt *et al*., « After Snowden : Rethinking the Impact of Surveillance », *International Political Sociology*, n. 8, 2014, 136.
[91] Malik, Mohan, « Technopolitics : How Technology Shapes Relations Among Nations », dans Watson, Virgina Bacay. *The Interface of Science, Technology & Security : Areas of Most Concern, Now and Ahead*, Asia-Pacific Center for Security Studies, 2012, 22.

Défense par la reproduction d'une logique de front militaire dans le domaine cyber[92]. Or, si le cyberespace est à la fois « nulle part et partout[93] », cela signifie que la tentative de l'encadrer au sein d'une infrastructure de surveillance se généralise à l'ensemble des données personnelles – autrement dit, la sécurité nationale américaine englobe *de facto* l'étendue globale du cyberespace : « Les prévisions indiquent que les avancées en recherche et développement vont transformer le champ de bataille dans les décennies à venir. […] Le 'front' va disparaître tandis que le pays entier deviendra le champ de bataille[94] ». Les stratégies étatiques consistent notamment à « intégrer le secteur privé dans ses objectifs en tant que fournisseur de renseignement sur les consommateurs […] [et à] annexer les systèmes d'information corporatifs au sein d'une infrastructure d'information sécurisée[95] ». Dans un contexte post-11-Septembre où prévaut l'impératif de sécurité nationale, les compagnies qui offrent des services majeurs dans le cyberespace sont légalement contraintes de coopérer avec les agences de renseignement. C'est notamment le cas dans cadre du programme PRISM[96], qui implique de grandes entreprises de la Toile comme Google, Facebook et Yahoo!. En définitive, cette superposition des agences de renseignement américaines au-dessus des grandes corporations, dont le modèle d'affaires repose déjà sur la marchandisation des données collectées au sujet de leurs utilisateurs, conduit à une structure en deux temps qui est vouée au suivi des citoyens et des non-nationaux sur la base de leurs traces numériques[97].

Enfin, la nébuleuse de surveillance étatique-corporative s'inscrit dans le contexte de l'émergence d'une gouvernance néolibérale globalisée[98]. En effet, de nombreuses activités de surveillance des données sont sous-traitées à des entreprises multinationales, donnant lieu selon Bauman à une autonomisation de la raison d'État, devenue hybride et globale au moment de s'étendre au-delà des responsables politiques vers les élites technocratiques :

> […] nous voyons la transformation de la raison d'État à travers l'émergence, [d'une part], d'une raison d'État numérisée et exercée par un complexe hétérogène de professionnels, [et d'autre part], d'information sensible hybridant les acteurs privés et

[92] Post, David, « Governing Cyberspace », *The Wayne Law Review*, vol. 43, n. 1, 1996, 160.
[93] Perry Barlow, John, « A Declaration of the Independence of Cyberspace », *Electronic Frontier Foundation*, 1996, URL : www.eff.org/cyberspace-independence (consulté le 4 décembre 2017).
[94] Malik, Mohan, « Technopolitics : How Technology Shapes Relations Among Nations », 22.
[95] Ball, Kirstie et David Murakami Wood, « Editorial : Political Economies of Surveillance », 2-3.
[96] Le programme PRISM sera abordé en détail au chapitre trois.
[97] Clarke, Roger, « Information technology and dataveillance », *Communications of the ACM*, vol. 31, n. 5, 1988, 498.
[98] Ball, Kirstie et David Murakami Wood, « Editorial : Political Economies of Surveillance », 3.

> publics. La nature transnationale de la collecte d'information qui traverse les frontières des États dissocie la nature discursive et homogène des intérêts de sécurité nationale tout en reconstruisant un agrégat de professionnels. […] Il pourrait être suggéré sans aller trop loin que ce que nous appelons encore la sécurité nationale a été colonisée par une nouvelle noblesse d'agences de renseignement opérant dans une arène transnationale de plus en plus autonome[99].

En somme, on constate que les transformations des pratiques de surveillance reflètent à la fois les tendances plus larges de l'économie politique – globalisation, privatisation et numérisation – ainsi que les caractéristiques des technologies informatiques – extension, intégration et modulation. Spécifiquement, la nature intégrée et l'absence de frontière dans le cyberespace signifient que les processus de surveillance se déploient autant à l'intérieur qu'à l'extérieur du pays, érodant la distinction historique entre les compétences régaliennes internes et externes. Cette situation, qui conjugue les notions de pouvoir, de sécurité, de surveillance et de population, est l'objet de plusieurs réflexions théoriques visant à conceptualiser ces nouvelles dynamiques.

1.1.3.3. Notion théorique : la gouvernementalité libérale

Dans le domaine multidisciplinaire des études de surveillance, les apports de Michel Foucault traitant de la relation entre le pouvoir et le savoir représentent une pierre angulaire à partir de laquelle s'ancre la littérature[100]. Une notion est particulièrement prégnante pour comprendre à la fois l'exercice du pouvoir dans les régimes libéraux ainsi que la structure participative et la fonction productive de la surveillance des données personnelles : la gouvernementalité.

D'abord, le néologisme « gouvernementalité » est défini par Foucault comme étant :

> l'ensemble constitué par les institutions, les procédures, analyses et réflexions, les calculs et les tactiques qui permettent d'exercer cette forme bien spécifique, quoique très complexe, de pouvoir, qui a pour cible principale la population, pour forme majeure de savoir l'économie politique, pour instrument technique essentiel les dispositifs de sécurité[101].

Historiquement, la gouvernementalité est associée à la conception moderne du pouvoir, où celui-ci ne provient pas de la conquête territoriale, mais plutôt de la mise en valeur des richesses

[99] Bauman, Zygmunt *et al*., « After Snowden : Rethinking the Impact of Surveillance », 126.
[100] Murakami Wood, David, « Editorial : Foucault and Panopticism Revisited », *Surveillance & Society*, vol. 1, n. 3, 235.
[101] Foucault, Michel, *Security, Territory, Population*, Palgrave MacMillan, 2009, 107-108.

nationales de sorte à accroître la productivité du territoire et de la population[102]. À ce titre, il serait possible de situer l'essor de la gouvernementalité libérale dans la période d'industrialisation, de pacification territoriale et d'expansion coloniale des puissances européennes entre 1815 et 1914[103].

La gouvernementalité libérale est concernée par le « problème de l'accumulation des hommes[104] » et cherche à agir sur les conditions de leur organisation et de la formation de leurs attitudes et de leurs comportements. Puisque la conception libérale du pouvoir suppose des limites claires aux prérogatives gouvernementales ainsi que des droits et des libertés aux individus, les stratégies de gestion des populations ne peuvent procéder simplement par la contrainte. En d'autres mots, comme les États libéraux présupposent et produisent un certain degré d'autonomie et de liberté chez chaque individu, la gouvernementalité doit s'exercer, non pas à l'encontre, mais à travers la liberté individuelle. La gouvernementalité libérale vise donc à produire des sujets adaptés à une liberté normalisée qui soit compatible avec les intérêts du système politique, économique et technique. Dans les États libéraux, ce processus dépend de la production de discours et de l'organisation d'incitatifs matériels qui soient appuyés par des systèmes de connaissances, en particulier les disciplines scientifiques, la police, la bureaucratie et les agences de surveillance[105].

Ces ensembles techniques et discursifs opèrent sur une logique rationnelle et empirique pour stimuler leur internalisation par la population, qui utilise dès lors son autonomie pour adapter et normaliser ses propres comportements. Ainsi, si la gouvernementalité libérale s'est développée d'abord dans les stratégies des États libéraux, elle ne saurait s'y réduire : la gouvernementalité fait référence à tout système qui opère une « conduite des conduites » en s'adressant aux intérêts rationnels de l'individu, comme la santé, la sécurité et la prospérité. En somme, en connectant les circuits de production de savoir et les structures d'exercice du pouvoir, la gouvernementalité consiste à « arranger les choses de façon à ce que la population, en ne suivant que son intérêt

[102] Lascoumes, Pierre, « La Gouvernementalité : de la critique de l'État aux technologies du pouvoir », *Le Portique*, n. 3-4, 2004, URL : http://leportique.revues.org/625#abstract (consulté le 4 décembre 2017).
[103] Anderson, Sheldon, « Metternich, Bismarck, and the Myth of the ''Long Peace'', 1815-1914 », *Peace & Change*, vol. 32, n. 3, juillet 2007, 301.
[104] Foucault, Michel, *Power/Knowledge: Selected Interviews and Other Writings*, Vintage Books, 1980, 151.
[105] Crampton, W. Jeremy, *The Political Mapping of Cyberspace*, 126.

propre, agisse comme elle le doit[106] », c'est-à-dire que la population réponde volontairement, dans l'agrégat, aux besoins systémiques des organisations politiques, économiques et techniques, particulièrement en matière de reproduction, de productivité, de pacification et de santé publique[107].

L'utilité du concept de gouvernementalité est d'appréhender la complexité du contrôle social dans les sociétés libérales, qui passe par l'organisation d'un espace de liberté qui soit limité par des lois, régulé par des discours normatifs, structuré par des incitatifs calculés et traversé par un principe d'économie du pouvoir. Ce système à la fois présuppose et produit l'individu en tant qu'acteur rationnel, dont la liberté est conçue comme une capacité à choisir les options les plus favorables. En arrangeant les incitatifs de façon à ce que la population agisse conformément aux intérêts des structures politiques et économiques, la gouvernementalité organise l'espace de liberté de sorte que les options les plus rationnellement favorables pour l'individu soient bénéfiques ou utiles aux organisations politiques, économiques ou techniques en question. Dans ce contexte, le rôle de la surveillance est, d'une part, de vérifier quelles options sont effectivement choisies par les individus – dans l'optique d'une sanction rétroactive – et d'autre part, de produire des savoirs sur les réalités sociales en vue de réformer les structures discursives et incitatives vers une plus grande efficience. La surveillance sert donc des fins inclusives et exclusives[108].

La relation circulaire entre le savoir et le pouvoir est au coeur de l'économie politique moderne : « La surveillance, en tant que mobilisation du pouvoir administratif – par la conservation et le contrôle de l'information – est le moyen principal de concentration des ressources autoritaires impliquées dans la formation de l'État-nation[109] ». Toutefois, la surveillance, de même que la gouvernementalité à laquelle elle peut contribuer, est aussi le fait de grandes entreprises, de systèmes technologiques et d'institutions en tous genres.

[106] Scott, David, « Colonial Governmentality », *Social Text*, n. 43, 1995, 202.
[107] Wiedner, Jason, « Governmentality, Capitalism and Subjectivity », *Global Society*, vol. 23, n. 4, octobre 2009, 389.
[108] Lascoumes, Pierre, « La Gouvernementalité : de la critique de l'État aux technologies du pouvoir ».
[109] Giddens, Anthony, *The Nation-State and Violence : Volume Two of a Contemporary Critique of Historical Materialism*, Polity Press, 1985, 181.

1.1.3.4. Une littérature empiriquement lacunaire

Manifestement, la littérature sur la surveillance incorpore des approches issues de la sociologie historique et de l'économie politique, où les réflexions posées par Michel Foucault prennent une place considérable. Le champ académique propose aussi des contributions conceptuelles originales, notamment en ce qui concerne la nébuleuse de surveillance étatique et corporative et l'assemblage surveillant. Toutefois, les perspectives analytiques demeurent souvent théoriques en ce qui concerne les comparaisons de la surveillance commerciale avec la surveillance sécuritaire.

1.1.4. Lacune analytique et question spécifique de recherche

La contribution du mémoire a pour objectif de pallier cette lacune constatée dans la littérature par une description et une comparaison empiriques des dimensions commerciale et sécuritaire de la surveillance des données personnelles. De cette façon, il sera possible de dégager les différences, les similitudes et les nuances au cœur de la nébuleuse de surveillance étatique et corporative. À cette fin, il s'agira d'étudier deux cas typiques, à savoir la surveillance commerciale pratiquée par l'entreprise Google et la surveillance sécuritaire pratiquée par la NSA. Étant donné que les deux organisations sont prééminentes dans leurs champs respectifs, elles constituent un axe propice à l'avancement empirique de la notion d'une nébuleuse étatique et corporative.

La question spécifique de recherche à laquelle nous entendons répondre est la suivante : quels sont les aspects convergeant et divergeant entre les contextes, les cibles, les principes, les tactiques et les stratégies de surveillance des données personnelles de l'entreprise Google et de la NSA?

1.1.5. Concepts

Certains concepts doivent être explicités en raison de leur centralité au sein des deux études de cas et de la comparaison analytique : la « nouvelle surveillance » et ses spécificités spatio-temporelles ainsi que le principe de « mise en données » sur lequel repose la gestion administrative des réalités sociales.

1.1.5.1. « Nouvelle surveillance » et surveillance des données

En raison de sa transformation récente ainsi que de sa généralisation, la surveillance est de plus en plus difficile à définir[110]. Néanmoins, il est clair que la définition classique offerte par le dictionnaire d'Oxford, soit l'observation attentive d'une personne suspecte[111], est dépassée de maintes façons par les nouvelles réalités sociotechniques. À ce titre, le chercheur canadien David Lyon la définit comme étant « toute attention systématique, routinière et concentrée aux détails personnels dans un but donné[112] ». Cette conception flexible a l'avantage de correspondre à l'aspect « liquide[113] » de la surveillance des données, qui opère de façon invisible, sur des flux de données en continu, au profit d'organisations informationnelles en constante évolution et d'individus organisés en réseaux.

C'est précisément la systématisation, la technicisation et l'automatisation de la surveillance, permises par la structure cybernétique du cyberespace, qui sous-tendent la « surveillance des données » (*dataveillance*[114]). Si l'informaticien Roger Clarke est à l'origine de ce terme, nous reprendrons toutefois la définition plus spécifique qui en est faite par la chercheuse Sara Degli Esposti :

> Le contrôle systématique de populations ou de groupes, au moyen de systèmes de gestion d'information numérique, dans le but de réguler ou gouverner leurs comportements […]. La surveillance des données peut être considérée comme un ensemble complexe de technologies et de pratiques sociales qui participent au changement sociotechnique général[115].

Ainsi, par opposition à la surveillance traditionnelle, qui s'établissait avec des intentions spécifiques, la surveillance des données implique le suivi continuel des données et métadonnées à des fins non spécifiées au préalable[116]. Or, la versatilité intrinsèque aux ressources informationnelles fait en sorte que la surveillance se généralise en tant que pratique sociotechnique et intègre progressivement le tissu social, ce qui fait de la surveillance des

---

[110] Marx, Gary, « What's New About the ''New Surveillance''? Classifying for Change and Continuity », *Surveillance & Society*, vol. 1, n. 1, 10.
[111] Oxford University Press, *Surveillance*, 2016, URL : http://www.oxforddictionaries.com/definition/english/surveillance (consulté le 4 décembre 2017).
[112] Lyon, David, *Surveillance Studies : An Overview*, Polity Press, 2007, 13.
[113] Lyon, David, « Liquid Surveillance : The Contribution of Zygmunt Bauman to Surveillance Studies », *International Political Sociology*, n. 4, 2010, 325.
[114] Clarke, Roger, « Information Technology and Dataveillance », 498.
[115] Degli Esposti, Sara, « When Big Data meets dataveillance : the hidden side of analytics », *Surveillance and Society*, vol. 12, n. 2, 210.
[116] Van Dijck, José, « Datafication, Dataism and Dataveillance : Big Data between scientific paradigm and ideology », 205.

données un phénomène dépassant le simple acte de scrutation des individus[117]. Notamment, son ascendance au sein des stratégies et tactiques économiques et politiques amène des problématiques importantes au contrat social, puisqu'elle altère la balance du pouvoir entre, d'un côté, les grandes entreprises technologiques et les agences gouvernementales et de l'autre, les citoyens et usagers[118].

L'appellation « nouvelle surveillance[119] » fait référence à ces changements récents et profonds du phénomène. Elle est intimement liée à ce que le philosophe Gilles Deleuze nomme la société du contrôle, qui succède historiquement à la société disciplinaire des 17e et 18e siècles. Alors que la discipline consiste à figer les corps au sein d'espaces fermés (écoles, hôpitaux, prisons, etc.) dans les logiques du *nation-building* et du *state-building*, le contrôle reflète les dynamiques de globalisation néolibérale en vérifiant à distance les comportements et attitudes de corps mobiles[120] situés dans une multitude de réseaux et visualisés sous la forme d'information[121].

En somme, la « nouvelle surveillance » peut être caractérisée par le fait que son contexte, ses outils, ses pratiques et ses objectifs sont rattachés aux dynamiques de l'économie politique. Il est alors possible de concevoir le complexe de technologies et de pratiques sociales[122] qui sous-tend la surveillance des données comme un épiphénomène de la mondialisation néolibérale et de l'essor du capitalisme informationnel.

1.1.5.2. Mise en données et lisibilité du social

Évidemment, la surveillance des données serait une pratique vouée à la non-pertinence s'il n'existait pas un complexe de technologies et de pratiques sociales axé sur la production continuelle de données. En ce sens, la surveillance des données dépend presque entièrement du processus de « mise en données » (*datafication*) ». Il s'agit essentiellement d'une numérisation –

[117] Andrejevic, M., « Exploitation in the data-mine », chapitre dans C. Fuchs, K. Boersma, A. Albrechtslung et M. Sandoval, *Internet and Surveillance : The Challenges of Web 2.0. and Social Media*, Routledge, 86.
[118] Van Dijck, José, « Datafication, Dataism and Dataveillance : Big Data between scientific paradigm and ideology », 205.
[119] Simon, Bart, « The Return of Panopticism : Supervision, Subjection and the New Surveillance », *Surveillance & Society*, vol. 3, n. 1, 1.
[120] Ruffolo, V. David, « Rhizomatic Bodies : Thinking through the Virtualities of Control Societies », *Rhizomes*, n. 17, 2008, URL : www.rhizomes.net/issue17/ruffolo.html (consulté le 4 décembre 2017).
[121] Deleuze, Gilles, « Postscript on the societies of control », *October*, vol. 59, hiver 1992, 7.
[122] Degli Esposti, Sara, « When Big Data meets dataveillance : the hidden side of analytics », 210.

la conversion d'un contenu analogique en signal numérique – des différents aspects de la vie humaine, qui sont reproduits sous la forme de données informatiques standardisées et quantifiées : « Les lunettes de réalité augmentée de Google mettent en données le regard. Twitter met en données les pensées filantes. LinkedIn met en données les réseaux professionnels. […] Même les amitiés et les 'appréciations' sont mises en données, via Facebook[123] ». Le potentiel économique et politique de ce processus est considérable, puisqu'il permet aux puissances politiques et économiques d'accéder en profondeur à de multiples dimensions de la réalité sociale qui étaient précédemment inaccessibles[124].

La mise en données suit logiquement des innovations numériques datant des années 1970, mais également du projet civilisationnel de la modernité scientifique, c'est-à-dire la quantification et la maîtrise de l'environnement naturel et social[125]. Il y a lieu de concevoir la mise en données avant tout comme une technologie de lisibilité, dont le fonctionnement est destiné à rendre les individus, leurs activités et leurs interactions « lisibles » pour un ensemble d'institutions et d'organisations[126] :

> La lisibilité est une condition de la manipulation. Toute intervention substantielle de l'État dans la société […] requiert l'invention d'unités visibles. […] Peu importe les unités étant manipulées, elles doivent être organisées d'une façon qui permette de les identifier, de les observer, de les enregistrer, de les compter, de les agréger et de les surveiller. En d'autres mots, il est possible d'affirmer que plus la manipulation envisagée est importante, plus la lisibilité nécessaire pour l'effectuer est grande[127].

Dans le contexte de la lisibilité sociale permise par la mise en données, la « lecture » effectuée ne porte pas directement sur les individus eux-mêmes, mais sur un assemblage de leurs traces numériques qui constituent un « sosie de données[128] » (*data double*). Cette méthode pose certains problèmes d'ordre épistémologique, puisque contrairement à la surveillance des individus, la surveillance de leurs données se base sur une production artificielle qui est séparée

---

[123] Neil Cukier, Kenneth et Viktor Mayer-Schoenberger, « The Rise of Big Data – How It's Changing the Way We Think About the World », *Foreign Affairs*, mai-juin 2013, URL : https://www.foreignaffairs.com/articles/2013-04-03/rise-big-data (consulté le 4 décembre 2017).
[124] Neil Cukier, Kenneth et Viktor Mayer-Schoenberger, « The Rise of Big Data – How It's Changing the Way We Think About the World ».
[125] Neil Cukier, Kenneth et Viktor Mayer-Schoenberger, « The Rise of Big Data – How It's Changing the Way We Think About the World ».
[126] Taylor, Linnet, « Data subjects or data citizens : Adressing the global regulatory challenge of big data », chapitre dans Mireille Hildebrandt et Bibi van den Berg, *Information, Freedom and Property : The Philosophy of Law Meets the Philosophy of Technology*, Routledge, 2016, 83.
[127] Scott, C. James, *Seeing Like A State : How Certain Schemes to Improve the Human Condition Have Failed*, 183.
[128] Lyon, David, « Surveillance, Snowden, Big Data – Capacities, Consequences, critique », 6.

de son contexte. De plus, la médiation technologique de la surveillance implique que les réalités et les activités qui ne peuvent pas être mises en données sont écartées du spectre des considérations[129]. En outre, le sosie de données produit par les technologies informatiques et réticulaires ne correspond jamais exactement à l'individu réel, mais constitue plutôt une heuristique utile aux organisations étatiques et commerciales.

1.2. Cadre méthodologique

Au vu de la complexité des rapports sociotechniques impliqués dans l'économie politique des données numériques, il est nécessaire d'employer une posture méthodologique suffisamment flexible pour s'appliquer à une configuration de pouvoir émergente[130] dans un environnement sociotechnique régi un rapport au temps et à l'espace distinct du réel[131]. C'est en ce sens que l'approche idiographique est préférée.

1.2.1. Objectifs

La recherche a pour objectif de contribuer à la compréhension du rôle de la surveillance des données aux structures des pouvoirs corporatifs et étatiques dans le cyberespace[132]. Ce faisant, il est envisagé de faire avancer la littérature sur la surveillance tout en développant une réflexion sur le pouvoir technologique qui aille au-delà des oppositions binaires entre la liberté et la sécurité ainsi qu'entre l'autonomie et le contrôle.

1.2.2. Stratégie descriptive

D'abord, nous procéderons à deux études de cas : la première portant sur l'entreprise Google et la seconde portant sur la NSA. La structure et la séquence des études de cas visent à étudier successivement les trois groupes d'acteurs de l'économie politique des données numériques dans un ordre d'autorité croissant : les populations qui génèrent des données en étant actives dans le cyberespace, les corporations qui structurent les plateformes et capitalisent sur les données et,

---

[129] Powell, A., « 'Datafication', Transparency, and Good Governance of the Data City », chapitre dans K. O'Hara, M-H. C. Nguyen et P. Haynes, *Digital Enlightenment Yearbook 2014 : Social Networks and Social Machines, Surveillance and Empowerment*, IOS Press, 2014, 223.

[130] Lyon, David, « Cyberspace sociality », chapitre dans Brian Loader, *The Governance of Cyberspace: Politics, Technology and Global Restructuring*, Routledge, 1997, 33.

[131] Highham, Pam, « Keeping it real : A critique of postmodern theories of cyberspace », chapitre dans Jose Lopez et Garry Potter, *After Postmodernism : An Introduction to Critical Realism*, A&C Black, 2005, 167.

[132] Bélanger, André-J, « Épistémologues de la science politique à vos marques! », chapitre dans Lawrence Olivier, Guy Bédard et Jean-François Thibault, *Épistémologie de la Science Politique*, Presses de l'Université du Québec, 1998, 24.

finalement, les agences de renseignement qui interceptent, filtrent et croisent ces données pour divers objectifs administratifs et politiques[133]. Ainsi, nous amorcerons chacune des deux études de cas par une description des activités des usagers qui croisent les intérêts et pratiques de l'organisation en question. Cette méthode vise à dresser un portrait du terrain social sur lequel s'établissent les processus de surveillance des données de Google et de la NSA. La suite des deux études de cas sera vouée à la description de quatre dimensions de la surveillance pratiquée par les deux organisations : les types d'information ciblés, les principes qui structurent la surveillance, les tactiques d'opération de la surveillance et, finalement, les stratégies servies par la surveillance. Cette stratégie descriptive répond donc à cinq questions : « qui ? », « quoi ? », « selon quelle rationalité ? », « comment ? » et « pourquoi ? ».

Ensuite, le dernier chapitre sera l'occasion de procéder à l'interprétation théorique de ces réponses en les reliant aux notions de « nébuleuse de surveillance étatique-corporative », de gouvernementalité et de conditionnement technologique. Ce faisant, nous comparerons les deux organisations entre elles sur la base des cinq dimensions descriptives afin d'en souligner les convergences et les divergences, conformément à notre question de recherche.

1.2.4. Instrument de collecte de l'information

La description des pratiques de surveillance des données de Google et de la NSA sera effectuée par observation documentaire. Cet instrument de collecte est adapté à l'opacité organisationnelle de nos cas d'étude, qui impose un recours important à la littérature scientifique et à la production médiatique. La littérature utilisée provient des réflexions académiques et multidisciplinaires des études de la surveillance[134]. L'instrument choisi répond manifestement aux critères de réactivité et de facilité d'accès. La fiabilité et la validité des résultats, quant à eux, dépendent surtout d'un échantillonnage efficient lors des études de cas. Quant aux enjeux éthiques liés à l'observation de documents diffusés illégalement par Edward Snowden, nous croyons qu'ils soient atténués par leur caractère désormais public[135], par l'aspect global de

[133] Lyon, David, « Surveillance, Snowden, Big Data – Capacities, Consequences, Critique », 3.
[134] Surveillance & Society, *Journal History*, 2016, URL : http://library.queensu.ca/ojs/index.php/surveillance-and-society/about/history (consulté le 4 décembre 2017).
[135] American Civil Liberties Union, *NSA Documents Released to the Public Since June 2013*, URL : www.aclu.org/nsa-documents-released-public-june-2013 (consulté le 4 décembre 2017).

l'enjeu soulevé ainsi que par l'intérêt élevé de ces informations pour la recherche en science politique. Dans l'étude du cas de Google, nous utiliserons une variété de monographies et d'articles scientifiques en plus des documents disponibles auprès de l'entreprise elle-même. Quant à l'étude des pratiques de la NSA, nous aurons recours à une pluralité d'articles scientifiques, à la monographie de Glenn Greenwald, le journaliste initialement contacté par Edward Snowden, ainsi qu'aux dossiers médiatiques organisés par les journaux *The Guardian* et *The Washington Post*. Évidemment, la description des pratiques de surveillance des données commerciales et sécuritaires peut requérir l'emploi d'autres sources documentaires selon les besoins épistémiques.

1.2.5. Cadre spatio-temporel

La recherche porte sur deux instances majeures de surveillance des données relatives à l'économie politique des données numériques : Google et la NSA. Étant donné la récence de cette configuration de pouvoir, le cadre temporel de la recherche se situe entre 2010 et 2013. Ces bornes sont pertinentes puisqu'elles incluent l'ascendance du « web 2.0 » chez les usagers de même que les fuites d'Edward Snowden au sujet des programmes de surveillance de la NSA.

Bien que notre contexte théorique et nos études de cas soient fermement ancrés dans le cadre du pouvoir structurel de l'hégémonie technoscientifique américaine[136], le caractère global du cyberespace fait de notre objet d'étude un phénomène éminemment transnational et diffus. Donc, nonobstant l'origine et la culture étasuniennes de Google et de la NSA, ces derniers entretiennent des politiques dans des espaces physiques et virtuels qui s'étendent bien au-delà des frontières des États-Unis.

1.2.6. Objectivation et considérations

En ce qui concerne l'objectivation du chercheur, il est entendu que la recherche procède d'un intérêt pour l'adaptation du pouvoir et du contrôle aux modalités d'une technologie comprime le temps et l'espace. Selon la typologie proposée par Martin Dodge et Rob Kitchin pour classer les paradigmes analytiques de l'étude du cyberespace, nous nous situons dans une perspective d'économie politique plutôt que du constructivisme social ou de l'utopisme : « L'analyse est donc centrée sur l'identification et l'explication de la relation entre le cyberespace et le capital,

[136] Krige, John, *American Hegemony and the Postwar Reconstruction of Science in Europe*, The MIT Press, 2008, 2.

et à tracer les manifestations sociales, politiques et économiques d'une telle relation[137] ». En effet, la recherche découle d'une perspective sociopolitique de la surveillance dans le cyberespace. L'imbrication globale, technocratique et profonde de l'économie politique des données numériques à la réalité sociale appelle à de nouvelles réflexions et contributions relatives à son incidence sur le cadre libéral et polyarchique des sociétés occidentales.

Toutefois, cette recherche ne prétend pas répondre de façon définitive à cette question. Au contraire, l'étude du cyberespace cautionne une attention particulière portée à sa réalité diffuse et changeante[138]. L'objectif de la recherche et de contribuer empiriquement à la notion d'une « nébuleuse de surveillance étatique-corporative » par une étude comparée de la surveillance des données pratiquée par Google et la NSA, tout en demeurant vigilant par rapport à la contingence de nos résultats. Nous voulons observer les pratiques effectives de la surveillance des données, les comparer entre elles, puis analyser leur relation avec les tendances de la modernité technoscientifique et de l'économie politique libérale.

La pertinence de la recherche est axée sur la récence de l'essor de la surveillance des données. En effet, il ne fait aucun doute que le 21^{e} siècle puisse être caractérisé par l'intégration croissante du cyberespace aux interactions socioculturelles et politico-économiques quotidiennes. Cette situation implique l'organisation et la régulation d'un nouvel espace d'action et de représentation, dont les implications personnelles, sociales et sociétales sont considérables, bien qu'encore peu étudiées[139].

> En bref, des domaines qui s'étendent du commerce aux communications en passant par les infrastructures critiques qui soutiennent la civilisation moderne opèrent tous sur ce qui est devenu un réseau des réseaux globalisé. […] Tout comme les bénéfices du domaine cyber se répercutent dans le domaine physique, avec des conséquences rapides et souvent inattendues, ainsi en est-il des inconvénients[140].

La recherche soutient l'importance majeure de réfléchir sur les dynamiques et les tendances politiques qu'implique la régulation informelle du cyberespace par un réseau d'agences de renseignement et de corporations opaques. En ce sens, l'avancement de la compréhension des modalités qui structurent le pouvoir dans le cyberespace est pertinent pour une pluralité de

[137] Dodge, Martin et Rob Kitchin, *Mapping Cyberspace*, Routledge, 2003, 26.
[138] Paul Marshall, Jonathan, *Living on Cybermind: Categories, Communication, and Control*, Peter Lang, 2007, 142.
[139] Idhe, Don, *Bodies in Technology*, University of Minnesota Press, 2002, 3-4.
[140] Singer, P. W. et Allan Friedman, *Cybersecurity and Cyberwar – What everyone needs to know*, Oxford University Press, 2014, 2.

disciplines académiques, pour la société civile ainsi que pour la viabilité du cyberespace lui-même, puisqu'il peut contribuer indirectement au projet d'émancipation caractéristique des approches critiques[141].

Comme les bases théoriques et méthodologiques de la recherche sont posées, il est maintenant possible de passer à la première étude de cas concernant la surveillance par l'entreprise Google.

[141] Bohman, James, « Critical Theory », dans *Stanford Encyclopedia of Philosophy* [en ligne], 2016, URL : http://plato.stanford.edu/entries/critical-theory/ (consulté le 4 décembre 2017).

Chapitre 2: Étude de cas des pratiques de surveillance des données de l'entreprise Google

Au chapitre précédent, nous avons présenté la problématique et la littérature scientifique relatives au phénomène de surveillance des données. Conformément à notre stratégie d'analyse descriptive, il s'agit maintenant de procéder à l'étude de cas des pratiques de surveillance des données de Google et de la NSA. Dans ce chapitre, nous décrirons le contexte, les cibles, les principes, les fonctions et les buts de la surveillance des données de Google, avant de conclure par une interprétation théorique des implications du modèle d'affaires de l'entreprise pour l'économie politique numérique.

2.1. Intersection des activités des usagers et des pratiques de surveillance des données de Google

La démocratisation du numérique a pour effet de dissiper graduellement les contraintes qui pesaient auparavant sur la création de contenu culturel, notamment en termes de coût de production et de restriction par les canaux de distribution. Comme la plupart des biens culturels sont véhiculés par le langage, les images et les sons, qui peuvent être numérisés, les créations culturelles deviennent de plus en plus faciles à produire, reproduire et distribuer[1]. Il en résulte une véritable prolifération qui se manifeste entre autres dans la popularité des blogues, de la baladodiffusion, des vidéos amateurs, des logiciels de transfert entre pairs, etc. Cette effervescence est en partie tributaire de la virtualité intégrative d'Internet, qui peut accommoder toute production culturelle en opposition aux politiques des grands groupes médiatiques qui régissaient les contenus à l'ère prénumérique.

Le passage de la rareté à l'abondance en matière de consommation médiatique et culturelle signifie que les individus du 21e siècle ont une liberté de choix inégalée en ce qui concerne les contenus qu'ils peuvent lire, visionner et écouter. La généralité du plus grand dénominateur commun est dépassée par l'émergence de milliers de « niches culturelles[2] » permises par la concentration du capital informationnel sur Internet et son accessibilité démocratique. Les individus peuvent créer et diffuser leur propre contenu, ce qui démocratise l'influence idéologique qui était jadis la chasse gardée des grandes organisations de l'industrie culturelle,

[1] Carr, Nicholas, *The Big Switch : Rewiring the World, from Edison to Google*, W.W. Norton & Company, 2008, 150-151.
[2] Gibson, Owen, « The Story of the Long Tail », *The Guardian*, 10 juillet 2006,
URL : https://www.theguardian.com/media/2006/jul/10/mondaymediasection5 (consulté le 15 mars 2017).

comme les chaînes télévisuelles et radiophoniques et les maisons de production cinématographique et musicale.

Donc, le 21e siècle amorce une réduction importante du pouvoir exercé par les intermédiaires médiatiques ainsi que la croissance parallèle de la liberté individuelle de produire, de diffuser et de consommer de l'information. C'est dans ce contexte que s'actualise la surveillance des données pratiquée par Google, qui est aussi tributaire de l'importance croissante assumée par le réseau Internet par rapport à l'ordinateur personnel des usagers. En d'autres mots, les ordinateurs sont de plus en plus comparables à des terminaux qui dérivent la majorité de leur utilité pratique du réseau Internet et des ordinateurs et des serveurs qui y sont branchés[3]. L'importance croissante des services de stockage infonuagique et des moteurs de recherche illustre le fait qu'une part importante des activités des usagers a lieu sur Internet, où Google jouit d'une prépondérance en matière de services populaires et d'affichage publicitaire.

En tant qu'archétype d'un nouveau modèle d'affaires, Google popularise de nombreuses innovations, non seulement dans ses services informatiques, mais aussi en matière de méthodes de travail, de gestion organisationnelle, de relations publiques et de ressources humaines[4]. Depuis 2015, la restructuration de l'entreprise a donné lieu à la création d'Alphabet, un conglomérat multinational regroupant différentes entreprises, dont Google, mais aussi Calico, CapitalG, DeepMind, GV, Verily et X[5]. Au sein de cette nouvelle structure, Google est épuré et axé sur sa gamme de produits destinés au grand public d'Internet, dont *Google Search*, *YouTube* et *Google Maps*.

En 2017, Google est une entité relativement incontournable pour l'usager typique d'Internet, qui recherche l'accessibilité et la performance[6]. Le moteur de recherche *Google Search* est un des

[3] Carr, Nicholas, *The Big Switch : Rewiring the World, from Edison to Google*, 17.
[4] Girard, Bernard, *The Google Way : How One Company is Revolutionizing Management as We Know It*, No Starch Press, 2009, 2.
[5] Calico est une entreprise de recherche et développement biotechnologique vouée à l'étude du vieillissement, de la dégénérescence neurale et du cancer ; CapitalG est une firme d'investissement à risque pour les entreprises technologiques étant au stade de croissance ; DeepMind est une entreprise concentrée dans l'intelligence artificielle et la création d'algorithmes d'apprentissage général ; GV est une firme d'investissement à risque pour les *start-ups* technologiques étant dans les premiers stades de conception ; Verily est une organisation de recherche vouée à l'étude des sciences de la vie ; X est une installation de recherche et développement vouée à l'innovation et aux projets financièrement risqués.
[6] Yusuf, Muhammad et Carl Adams, « A Base of Knowledge, Mobile, and Web 2.0 Technologies for Connected E-Government », chapitre dans Mahmood Zaigham, *Emerging Mobile and Web 2.0 Technologies for Connected E-Government*, IGI Global, 2014, 118.

piliers de l'entreprise et enregistre plus de 100 milliards de requêtes individuelles chaque mois[7]. À ce titre, *Google Search* est le service utilisé pour plus de 60 % des recherches faites aux États-Unis et plus de 90 % de celles faites en Europe[8]. En somme, Google opère à l'intersection des intentions des usagers et de l'information disponible sur Internet : cette position en recul signifie que l'usager qui soumet une requête à l'interface impersonnelle et automatisée de Google est susceptible d'y inscrire directement ses pensées, ses inquiétudes, ses réflexions et ses questionnements[9].

2.2. Types de données personnelles collectées, traitées et analysées par Google

La surveillance des données pratiquée par Google concerne un éventail d'informations qui, de manière agrégée, assemble des sosies de données approfondis. Selon les conditions d'utilisation de l'entreprise, celle-ci collecte des données liées, notamment, aux appareils, à l'utilisation des services, à l'emplacement géographique et aux témoins (*cookies*) de navigation. Puisque ces informations sont à la base des stratégies de surveillance de Google, il est pertinent de s'y intéresser de plus près.

Dans un premier temps, un pan de la collecte de données relève de la communication directe de certaines informations à l'entreprise lors de la création d'un compte Google, ce processus étant nécessaire à certains services (comme Google+) et fonctionnalités (comme pour mettre une vidéo en ligne sur YouTube). Ces données peuvent inclure le nom de l'usager, son adresse courriel, son numéro de téléphone ainsi que le numéro d'une carte de paiement, qui peut être utilisée pour attester de l'âge légal de l'usager. Dans un deuxième temps, le reste des informations est collecté par Google par l'entremise de l'usage de ses services, ce qui s'étend à la consultation de sites web qui utilisent les services publicitaires de Google.

Parmi ces informations, Google collecte des données relatives au matériel informatique utilisé pour accéder à ses services, incluant le modèle, le système d'exploitation, l'identifiant unique, le réseau mobile et, dans certains cas, le numéro de téléphone. Ces données peuvent ensuite être

---

[7] Google, *Inside Search – How Search Works – The Story*, 2017,
URL : https://www.google.ca/insidesearch/howsearchworks/thestory/ (consulté le 4 mars 2017).
[8] The Guardian, « Google dominates search. But the real problem is its monopoly on data », 19 avril 2015, URL : https://www.theguardian.com/technology/2015/apr/19/google-dominates-search-real-problem-monopoly-data (consulté le 15 avril 2017).
[9] Schneier, Bruce, *The Hidden Battles to Collect Your Data and Control Your World*, 22.

associées au compte Google de l'usager. Aussi, Google collecte et traite les données relatives à la position exacte des usagers, notamment à l'aide de l'adresse de protocole Internet[10], des signaux GPS, des points d'accès au Wi-Fi et des antennes-relais cellulaires.

Ensuite, Google collecte des « fichiers journaux », qui enregistrent la façon dont est utilisé un service : les requêtes de recherches effectuées, les liens et publicités cliqués, de même que les données d'usage[11], les préférences d'utilisation, les messages reçus ou envoyés par Gmail, le profil Google+, l'historique de recherche, les recherches cartographiques, ainsi que les photos, vidéos et autres documents hébergés par Google. Ces journaux incluent aussi l'adresse IP des usagers, de même que les rapports d'échecs, l'activité du système, les paramètres du matériel informatique, le type et la langue du fureteur utilisé, la date et l'heure des requêtes effectuées et l'adresse URL de référencement[12]. Ils incluent également les données relatives aux communications téléphoniques, comme le numéro de téléphone de l'usager, celui de l'appelant, les numéros de transfert, l'heure et la date des appels, leur durée, les métadonnées des messages textes et les types d'appels. Toutes ces données sont analysées automatiquement au moment de leur envoi, de leur réception et de leur stockage.

Finalement, Google et ses partenaires (dont des organisations de mesure d'audience et des chercheurs) utilisent des témoins informatiques pour identifier le fureteur et l'appareil de l'usager. Les témoins sont aussi utilisés pour collecter des informations à propos de la consultation des publicités et des fonctionnalités de Google sur d'autres sites web – comme le « +1 » de Google+. Avec *Google Analytics*[13], les clients de Google peuvent analyser le trafic de consultation de leurs sites web et applications. Lorsqu'ils combinent ce système avec les services publicitaires de Google, ces partenaires et clients peuvent associer les données de *Google Analytics* avec celles provenant de témoins de tiers partis[14]. Ce croisement permet d'inférer les comportements et intérêts répétés des usagers afin de « créer des annonces plus pertinentes ou

[10] L'adresse de protocole Internet est le numéro qui identifie un appareil connecté à l'Internet, attribuée par groupe géographique. L'adresse permet d'identifier la position géographique de l'appareil.
[11] Données relatives au temps passé sur un site web.
[12] Concerne l'adresse URL précédemment consultée par l'usager avant d'accéder à une nouvelle adresse.
[13] *Google Analytics* est un service gratuit d'analyse de l'audience d'un site web ou d'une application.
[14] Les témoins de tiers partis appartiennent généralement à des entreprises publicitaires. Contrairement aux témoins propriétaires, qui sont stockés par le site consulté et y demeurent confinés, les témoins de tiers partis suivent les différents sites consultés par un même usager.

d'analyser son trafic de manière plus approfondie[15] ».

Il est important de noter que les nombreuses données personnelles, bien que collectées à travers des applications, des services, des appareils et des technologies distinctes, peuvent ensuite être regroupées en vue de certaines fonctionnalités, de l'amélioration des services et de l'affinement des publicités diffusées par Google. Certains exemples de regroupement sont officiellement fournis par Google, dont l'utilisation des informations issues de la boîte de réception Gmail d'un usager pour lui fournir des notifications personnalisées, l'utilisation des données sur les relations sociales d'un compte Google+ pour faciliter la connexion par Gmail, ou encore l'utilisation des données provenant de l'historique de navigation pour raffiner les résultats des requêtes de recherche.

2.3. Les principes opératoires de la surveillance des données de Google

Les principes de la surveillance des données de Google sont liés aux spécificités de son modèle d'affaires hybride. En particulier, la surveillance des données de Google est structurée par les principes axiomatiques d'un marché biface : d'un côté, Google attire une masse critique d'usagers par l'économie du don[16], et de l'autre, l'entreprise capitalise sur cette masse d'usagers sur la base de l'économie de l'attention[17].

2.3.1. Surveillance des données : le marché biface et l'économie de l'attention

D'abord, un marché biface se caractérise par l'interdépendance de deux marchés au sein du modèle d'affaires d'une entreprise ou d'un service. Dans le cas d'un moteur de recherche comme Google, ces deux marchés sont ceux des usagers et des publicitaires : plus le nombre d'usagers de ses services est élevé, plus la valeur de ses produits publicitaires croît pour les entreprises et

[15] Google, *Règles de confidentialité*, 2017, URL : https://www.google.com/intl/fr/policies/privacy/ (consulté le 8 mars 2017).
[16] Relation économique qui repose sur un don apparent, mais réalisé dans l'attente de réciprocité sous une forme ou une autre. Dans ce cas-ci, Google fait le « don » de ses logiciels aux usagers, qui réciproquent à travers le « don » continuel des données personnelles créées ou captées par ces logiciels.
[17] Le passage d'un marché informationnel mené par l'offre (rareté) à un marché fondé sur la demande (abondance) signifie qu'un nombre croissant d'émetteurs d'information sont en compétition pour capter et maintenir l'attention cognitive des audiences.

agents de marketing[18]. D'un côté, Google organise l'espace publicitaire des sites web qui cherchent à rentabiliser la gratuité de leur information en tirant profit de l'attention et des intérêts de leurs visiteurs[19]. De l'autre côté, Google vend aux publicitaires l'espace des fournisseurs et l'attention des consommateurs, sa rémunération étant basée sur le « paiement par clic ». Bien que les journaux fonctionnent depuis longtemps sur un modèle similaire afin d'être compétitifs, le processus de sélection et d'affichage des publicités n'était pas centralisé entre les mains d'une organisation informationnelle d'envergure globale. La surveillance des données apparaît comme le point de contact majeur de l'entreprise avec les deux marchés qu'elle vise.

L'entretien de deux marchés aux intérêts distincts s'appuie sur l'effet de réseau, soit le cercle vertueux établi entre le nombre d'usagers d'un service et la valeur de ce service pour les usagers potentiels. En d'autres mots, le succès alimente le succès : plus les usagers de ses services sont nombreux et produisent de l'information, plus ses offres publicitaires gagnent en valeur et attirent les annonceurs[20] ; plus l'entreprise génère de revenus publicitaires, plus l'entreprise peut améliorer ses services et innover pour attirer davantage d'usagers[21]. La gratuité des services signifie que quiconque peut produire et publier du contenu, attirant ainsi des visiteurs et générant plus d'opportunités publicitaires pour Google[22]. Au centre de cette relation, la surveillance des données constitue le pont entre l'usage des services et la production d'une valeur exploitable.

2.3.2. Présence en amont, surveillance en aval : cybernétique de l'exploitation du contenu généré par les usagers

Les principes de la surveillance des données de Google procèdent d'une exploitation stratégique de la jonction entre les intérêts des usagers – accéder à des services efficients, gratuitement – avec ses propres intérêts organisationnels – accéder à de gigantesques volumes de données personnelles, vendre de la publicité, améliorer ses services et en créer des nouveaux. Dans cette situation, l'économie du don prend la forme d'un échange tacite entre l'accès aux services de

[18] Great Britain Competition Commission, *Classified Directory Advertising Services Provisional Findings*, The Stationery Office, 2006, 79.
[19] Luchetta, Giacomo, *Is The Google Platform a Two-Sided Market ?*, SSRN, 2012,
URL : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2048683 (consulté le 6 mars 2017).
[20] Fuchs, Christian, *Social Media : A Critical Introduction*, SAGE, 2013, 131.
[21] Lanier, Jaron, *Who Owns the Future*, Simon & Schuster, 2014, 170.
[22] Girard, Bernard, *The Google Way : How One Company is Revolutionizing Management as We Know It*, 29.

l'entreprise et l'accès aux données personnelles des usagers.

D'un côté, la gratuité apparente des services de Google réduit la barrière d'entrée à leur utilisation, ce qui stimule leur croissance et généralisation[23]. De l'autre côté, malgré l'absence de prix, les conditions d'utilisation de Google rappellent que le coût d'usage de ses services consiste en une surveillance permanente des usagers et de l'information qu'ils produisent : des « systèmes automatisés analysent [les] contenus (y compris les courriels) […] lors de l'envoi, de la réception et du stockage des contenus[24] ». Plus encore, cette logique de concession implique l'octroi d'une licence d'exploitation du contenu des usagers :

> Lorsque vous importez, soumettez, stockez, envoyez ou recevez des contenus à ou à travers de nos Services, vous accordez à Google (et à toute personne travaillant avec Google) une licence, dans le monde entier, d'utilisation d'hébergement, de stockage, de reproduction, de modification, de création d'œuvres dérivées, de communication, de publication, de représentation publique, d'affichage public ou de distribution publique desdits contenus[25].

Cette complémentarité entre la gratuité des services et la transaction d'information est centrale à la stratégie de l'entreprise. Elle reflète l'impératif majeur posé par la compétition entre les compagnies informatiques, qui diffère de celui de l'économie politique matérielle. Plutôt que de se spécialiser, l'impératif consiste à se généraliser en atteignant une position sociotechnique de premier ordre sur le plan de l'information[26]. Cette course à la « métaposition » donne aux plateformes l'apparence d'un service public[27], une impression renforcée par l'absence de prix et la réalité effective de l'utilisation répandue du service. En réalité, la valeur des données et informations générées au sein de ces services est entièrement accaparée par les intérêts techniques et commerciaux de Google. Le métapositionnement de l'entreprise – son rôle d'intermédiaire entre les usagers et l'information créée sur la Toile – est central à ses pratiques de surveillance des données.

La stratégie principale de Google est de ne pas produire de contenu, mais de se concentrer plutôt

---

[23] Girard, Bernard, *The Google Way : How One Company is Revolutionizing Management as We Know It*, 37.
[24] Google, *Conditions d'utilisation de Google*, 2014, URL : https://www.google.com/intl/fr/policies/terms/ (consulté le 6 mars 2017).
[25] Google, *Conditions d'utilisation de Google*.
[26] Lanier, Jaron, *Who Owns the Future*, 188.
[27] Fallows, James, « Facebook, Google, and the Future of the Online 'Commons' », *The Atlantic*, 3 février 2012, URL : https://www.theatlantic.com/technology/archive/2012/02/facebook-google-and-the-future-of-the-online-commons/252522/ (consulté le 8 mars 2017).

sur la création d'outils et de services qui encouragent la création de contenu par les usagers[28] : « Nos services affichent des contenus n'appartenant pas à Google[29] ». Cette pratique relève de la production participative (*crowdsourcing*), c'est-à-dire que la production de contenu sur le site repose sur les usagers, tandis que les externalités commerciales et culturelles de cette production sont la propriété exclusive de l'entreprise qui gère le fonctionnement technique des plateformes et services[30]. En d'autres mots, ce sont des milliers, voire des millions d'usagers non rémunérés qui, dans leurs interactions collectives, fondent et confèrent une valeur à une structure techno-économique extrêmement profitable pour un groupe restreint d'individus[31].

Cette dévolution complète du contenu peut parfois constituer une faiblesse en ce qui a trait à l'impératif publicitaire et analytique de maintenir l'usager sur la page des résultats de recherche de *Google Search*. Les usagers utilisent le moteur de recherche en vue de le quitter vers leur réelle destination. Cette faiblesse est vraisemblablement un des facteurs explicatifs de la rapide évolution de Google au-delà de son moteur de recherche, vers d'autres types de services qui reproduisent son métapositionnement et la dévolution de la production de contenu, tout en circonscrivant et conservant l'attention de l'usager[32] : les domaines sociotechniques des communications personnelles avec Gmail, des vidéos amateurs et professionnels avec *YouTube*, des reproductions géographiques, spatiales et routières avec *Google Earth* et *Google Maps*.

En se concentrant exclusivement sur les outils de production de contenu, Google opère au niveau de l'organisation de l'information, de son accessibilité et de son utilité[33], une métaposition précieuse sur les plans commercial et technique[34]. En effet, cette place en amont permet à Google de se placer entre l'information brute d'Internet et l'attention des usagers. Or, le principe d'interaction principal de cet intermédiaire avec les usagers et le contenu public du web est la surveillance des données. D'un côté, Google surveille, indexe et organise l'ensemble du contenu mis en ligne sur Internet : cette « métaposition » lui permet d'exploiter automatiquement – à

[28] Girard, Bernard, *The Google Way : How One Company is Revolutionizing Management as We Know It*, 37.
[29] Google, *Conditions d'utilisation de Google*.
[30] Carr, Nicholas, *The Big Switch : Rewiring the World, from Edison to Google,* 142-143.
[31] Carr, Nicholas, *The Big Switch : Rewiring the World, from Edison to Google*, 141-142.
[32] Girard, Bernard, *The Google Way : How One Company is Revolutionizing Management as We Know It*, 38.
[33] Google, *Our story – From the garage to the Googleplex*, 2017, URL : https://www.google.com/about/our-story/ (consulté le 8 mars 2017).
[34] McRae, Hamish, « Facebook, Airbnb, Uber, and the unstoppable rise of the content non-generators », *The Independent*, 5 mai 2015, URL : http://www.independent.co.uk/news/business/comment/hamish-mcrae/facebook-airbnb-uber-and-the-unstoppable-rise-of-the-content-non-generators-10227207.html (consulté le 8 mars 2017).

l'aide des logiciels d'indexation (*web crawlers*) – tout le contenu public en ligne sans rémunérer quiconque. De l'autre côté, les usagers qui emploient les services de Google acquiescent à participer indirectement au labeur de production de données commercialisables[35]. Grâce à la surveillance des données, les deux principales ressources dans lesquelles puise Google, soit l'information publique d'Internet et les données personnelles des usagers, lui sont directement accessibles sans relation contractuelle ni compensation.

2.4. Usages tactiques (fonctions) de la surveillance des données

La surveillance des données joue une pluralité de rôles au sein des différentes offres de produit de Google. Ces usages sont qualifiés de « tactiques », puisqu'ils réfèrent à des opérations contextuelles, adaptées et circonscrites aux structures et objectifs de chacun des services. Le grand nombre de produits offerts par Google – et le nombre encore plus élevé de tactiques de surveillance différenciées – en proscrit la description exhaustive et complète. Il importe surtout de saisir les ressorts centraux de la surveillance des données au sein des fonctionnalités techniques des services de Google. Pour ce faire, nous décrirons les tactiques relatives aux services prédominants de l'entreprise.

Le succès initial ainsi que l'innovation fondamentale du moteur de recherche de Google relèvent de la sophistication de son algorithme, *PageRank*[36]. Cet algorithme complexe et protégé par le secret commercial opère en tant qu'outil très avancé de surveillance des données. D'abord, ses logiciels d'indexation sillonnent en temps réel les pages publiques d'Internet, copient leur contenu et suivent les hyperliens qui y sont inscrits[37]. La répétition de ce processus mène à l'archivage des milliards de pages web copiées dans l'« index[38] » et traitées par *PageRank* lors de l'usage du moteur de recherche de Google[39]. Ensuite, *PageRank* détermine une valeur numérique de l'importance de la page en fonction, notamment, de la valeur des autres pages qui y mènent ;

---

[35] Fuchs, Christian, *Social Media : A Critical Introduction*, 131.
[36] Levy, Steven, « Exclusive : How Google's Algorithm Rules the Web », *Wired*, 22 février 2010, URL : https://web.archive.org/web/20110612022158/http://www.wired.com/magazine/2010/02/ff_google_algorithm/2 (consulté le 9 mars 2017).
[37] Google, *Technology Overview*, 4 juin 2011, URL : https://web.archive.org/web/20110604120221/http://www.google.com/about/corporate/company/tech.html (consulté le 9 mars 2017).
[38] L'*Index* est le nom donné à la copie de la Toile publique que Google entretient dans ses systèmes et sur laquelle se basent ses services de recherche.
[39] Google, *Inside Search – How Search Works – The Story*.

le processus par lequel les résultats d'une recherche sont ordonnés est donc récursif et itératif[40]. Aujourd'hui, plus de 200 signaux influencent l'ordre des résultats de *PageRank*, dont l'emplacement géographique de l'usager, son historique de navigation ainsi que le nombre de clics sur un résultat par d'autres usagers.

La double surveillance intrinsèque au fonctionnement du moteur de recherche Google, en ce qui a trait au contenu public de l'Internet et aux données personnelles des usagers de ses services, a déjà été décrite. Ces deux formes de surveillance convergent au sein de la principale source de revenus de l'entreprise, *AdWords*. Ce service publicitaire lancé en 2000 consiste en l'affichage contextuel de brèves annonces écrites[41]. Les annonceurs procèdent à des enchères entre eux, qui déterminent leur priorité d'affichage relativement à des mots-clés, et décident du prix par clic qu'ils désirent débourser[42]. Ces annonces sont affichées à côté des résultats de recherche des usagers dont les requêtes correspondent à ces mots-clés au sein de zones géographiques spécifiques[43]. Ce service publicitaire contextualisé peut s'étendre à travers les sites de l'entreprise[44], mais aussi à travers le *Google Display Network*, un groupe de plus de deux millions de vidéos, applications et sites web[45]. Donc, la surveillance des requêtes de recherche à travers ses services est la condition d'existence du système publicitaire *AdWords* de Google, puisque la collecte et l'analyse automatisées des requêtes permettent d'afficher des publicités contextualisées.

En parallèle au service *AdWords*, utilisé par les publicitaires, Google a introduit en 2003 un service destiné aux sites d'hébergement de contenu, *AdSense*. Celui-ci s'adresse aux sites qui désirent dériver un revenu de leur consultation en affichant des publicités *Ad Words* adaptées au contenu de leurs pages. Environ 14 millions de sites web[46] participent à ce programme et participent au réseau d'affichage des publicités *AdWords*. Le programme emploie des logiciels

[40] Fuchs, Christian, *Social Media : A Critical Introduction*, 132.
[41] Ayant un maximum de 140 caractères.
[42] Fuchs, Christian, *Social Media : A Critical Introduction*, 132.
[43] Girard, Bernard, *The Google Way : How One Company is Revolutionizing Management as We Know It*, 30.
[44] Comme *YouTube*, *Google Play*, *Google Shopping* et *Google Maps*, entre autres.
[45] Google, *AdWords Help – Setup and Basics – Where your ads can appear*, 2017, URL : https://support.google.com/adwords/answer/1704373?hl=en (consulté le 9 mars 2017).
[46] Built With, *Websites using Google AdSense*, 2017, URL : https://trends.builtwith.com/websitelist/Google-Adsense (consulté le 9 mars 2017).

d'indexation distincts de ceux relatifs à l'algorithme *PageRank*[47] pour identifier automatiquement les mots-clés et inférer le contenu des pages participantes. Chaque fois qu'un usager clique sur une publicité contextuelle, le détenteur du site web est rémunéré – cette façon de faire supporte la publication de contenu gratuit[48] tout en cadrant avec les intérêts techno-économiques du moteur de recherche de Google. Dans ce contexte, la surveillance des données est à première vue limitée au contenu des pages des sites participants, puisqu'il s'agit de la source effective du type de publicité affiché. Toutefois, en consultant des pages qui utilisent « les produits publicitaires (*AdSense*), les produits sociaux (comme le bouton +1), ou les produits analytiques (*Google Analytics*)[49] » de Google, les usagers partagent automatiquement certaines informations avec l'entreprise. Avec *AdSense*, Google utilise le témoin de tiers parti de *DoubleClick*, un de ses subsidiaires spécialisés dans les technologies publicitaires qui fut acquis en 2008 au coût de 3 milliards $. À travers la consultation des pages faisant affaire avec *AdSense*, *DoubleClick* peut placer des témoins sur les fureteurs des usagers et lire ceux qui y sont déjà présents[50]. Le produit de Google emploie donc la surveillance des données à deux niveaux principaux : celui du contenu des pages participant à *AdSense* et celui des informations contenues dans les témoins présents sur les fureteurs des usagers qui consultent ces pages.

2.5. Usages stratégiques (buts) de la surveillance des données

Au-delà des applications tactiques et fonctionnelles de la surveillance des données aux services et produits offerts par Google, celle-ci s'inscrit au sein de stratégies organisationnelles aux objectifs plus généraux. En tant qu'organisation capitaliste spécialisée dans l'information, Google vise naturellement à maximiser l'usage de ses ressources, la performance de ses services et son positionnement relatif à ses compétiteurs. Bien que ces objectifs stratégiques ne se réduisent pas à la surveillance des données, ils en soulignent les rôles généraux à l'échelle des intérêts organisationnels de l'entreprise.

---

[47] Google, *AdSense Help – Managing websites – About the AdSense crawler*, 2017, URL : https://support.google.com/adsense/answer/99376?hl=en (consulté le 9 mars 2017).
[48] Girard, Bernard, *The Google Way : How One Company is Revolutionizing Management as We Know It*, 38.
[49] Google, *Privacy & Terms – Partners – How Google uses data when you use our partners' sites or apps*, 2017, URL : http://www.google.com/policies/privacy/partners/ (consulté le 10 mars 2017).
[50] Un témoin inclut, entre autres, l'adresse de protocole Internet de l'usager et l'adresse URL de la page consultée.

2.5.1. Sécurité et efficience des services et algorithmes

Dans les communications de l'entreprise, il est affirmé que la collecte des données vise à « fournir, gérer, protéger et améliorer[51] » ses services. À titre d'exemple, Google mentionne que la collecte de données automatisée permet aux services de connaître la langue de l'utilisateur, les publicités les plus susceptibles de lui être utiles, les personnes qui lui sont le plus importantes et les vidéos *YouTube* les plus susceptibles d'être appréciées. L'entreprise affirme que la surveillance de ses systèmes, de ses services, des adresses IP et des témoins des usagers lui sert, entre autres, à s'assurer de leur fonctionnement optimal ainsi qu'à la protection contre les « abus automatisés[52] ».

Étant donné la centralité de l'information pour l'entreprise, l'usage de la surveillance des données est consubstantiel avec le raffinement des algorithmes de ses services. Ce raffinement s'inscrit au sein de sa stratégie commerciale visant à assembler, mettre à jour et approfondir des profils individuels. La transparence des usagers au sein des systèmes de gestion des connaissances de Google fut évoquée en 2010 par son PDG, Eric Schmidt. En parlant des possibilités technologiques à venir et des projets de Google relatifs à la réalité augmentée[53], il a souligné les aspects fonctionnalistes – et en partie volontaristes – de la surveillance des données personnelles :

> Avec votre permission, vous nous donnez plus d'information à propos de vous, à propos de vos amis, et nous pouvons utiliser cette information, encore une fois, avec votre permission, pour améliorer la qualité de nos recherches. […] Nous n'avons pas besoin que vous écriviez quoi que ce soit. Nous savons où vous êtes, avec votre permission. Nous savons où vous avez été, avec votre permission. Nous pouvons plus ou moins deviner ce à quoi vous pensez[54].

En somme, la surveillance est le procédé central de fonctionnement et de perfectionnement des services de Google. Le succès de l'entreprise est lié à la façon dont elle « met les usagers au

---

[51] Google, *Règles de confidentialité et conditions d'utilisation – Comment nous utilisons les données que nous collectons*, 2017, https://www.google.com/intl/fr/policies/privacy/ (consulté le 11 mars 2017).
[52] Google, *Règles de confidentialité et conditions d'utilisation – Comment nous utilisons les données que nous collectons*.
[53] Madrigal, Alexis, « The World Is Not Enough : Google and the Future of Augmented Reality », *The Atlantic*, 25 octobre 2012, URL : https://www.theatlantic.com/technology/archive/2012/10/the-world-is-not-enough-google-and-the-future-of-augmented-reality/264059/ (consulté le 11 mars 2017).
[54] Thompson, Derek, « Google's CEO : 'The Laws Are Written by Lobbyists' », *The Atlantic*, 1 octobre 2010, www.theatlantic.com/technology/archive/2010/10/googles-ceo-the-laws-are-written-by-lobbyists/63908/ (consulté le 4 mars 2017).

premier plan[55] » de sa stratégie commerciale. Conformément à la logique du marché biface, la croissance du nombre d'usagers de ses services et de l'information totale sur la Toile publique constitue des vecteurs de croissance de l'entreprise, par le biais de la surveillance des données et de la capitalisation qu'elle permet auprès des publicitaires. Donc, la surveillance des données personnelles, en tant que moyen principal d'accumulation de capital, permet à Google de disposer des ressources informationnelles et financières nécessaires à l'amélioration de ses produits ainsi qu'à la conception de nouveaux services. Cette boucle itérative signifie que la surveillance des données sert sa propre reproduction à travers de nouveaux cadres sociotechniques et fonctionnalités.

2.5.2. Entretien et croissance du marché publicitaire

En tant qu'entreprise basée sur les revenus publicitaires, Google emploie aussi la surveillance des données en tant que moyen de constitution principal du capital informationnel qu'elle commercialise[56]. Google jouit d'une position dominante au sein du marché des technologies publicitaires[57]. À ce titre, près de 90 % de ses revenus de 75 milliards $ US (2015) proviennent de ses activités publicitaires qui emploient la surveillance des données personnelles, dont au premier chef *AdWords* (69 %) et *AdSense* (20 %)[58]. Selon son rapport de l'année 2016, les produits de Google ont généré 222 milliards $ US d'activité économique pour 1,5 million d'entreprises, d'hébergeurs de sites et d'organisations sans but lucratif à l'échelle étasunienne[59].

La surveillance des données pratiquée par Google sur les usagers de ses services gratuits est à la base de son chiffre d'affaires, puisqu'elle fournit l'information permettant un ciblage personnalisé de la persuasion publicitaire ainsi que l'évaluation de son effet. Par exemple, le service *Google Analytics* visualise et quantifie la circulation en ligne en fournissant des informations, notamment, sur les usagers qui visitent un site, sur les pages qu'ils regardent et sur

---

[55] Girard, Bernard, *The Google Way : How One Company is Revolutionizing Management as We Know It*, 3.
[56] Fuchs, Christian, *Social Media : A Critical Introduction*, 132.
[57] Grunes, Allen, « Google's Quiet Dominance Over The 'Ad Tech' Industry », *Forbes*, 26 février 2015, www.forbes.com/sites/realspin/2015/02/26/googles-quiet-dominance-over-the-ad-tech-industry/#1e6d31215b78 (consulté le 4 mars 2017).
[58] Alphabet Investor Relations, *Press Release – Alphabet Announces Fourth Quarter and Fiscal Year 2015 Results*, 2016, URL : https://abc.xyz/investor/news/earnings/2015/Q4_google_earnings/index.html (consulté le 11 mars 2017). Pour les proportions relatives à *AdWords* et *AdSense*, voir : Rosenberg, Eric, « The Business of Google (GOOG) », *Investopedia*, 5 août 2016, URL : http://www.investopedia.com/articles/investing/020515/business-google.asp (consulté le 11 mars 2017).
[59] Google, *Economic Impact*, 2016, URL : https://economicimpact.google.com/#/ (consulté le 5 décembre 2017).

le temps passé sur chacune d'entre elles[60]. Le but de Google par rapport à ses produits publicitaires est de maximiser le *click-through rate*, c'est-à-dire le fait de cliquer sur une publicité après y avoir été exposé[61]. À cet égard, Schmidt a affirmé que « si nous [Google] présentons la bonne publicité à la bonne personne au bon moment et qu'elle clique dessus, nous gagnons[62] ». C'est notamment vers cette « victoire » que tend la surveillance des données personnelles, puisqu'il s'agit d'un processus essentiel à l'estimation des goûts, des préférences, des intérêts et des besoins des usagers des services de Google[63].

Le profilage sociodémographique et psychologique des usagers constitue une ressource informationnelle aux finalités inépuisables et fongibles. Cette ressource est utilisée, entre autres, pour permettre aux clients de Google d'optimiser leurs communications en segmentant celles-ci en fonction de critères spécifiques qui constituent des publics niches[64]. Ce faisant, Google internalise les coûts et l'infrastructure technique nécessaire à la collecte de renseignement sur un vaste ensemble de consommateurs, tandis que ses clients profitent d'une externalisation de ces coûts, ce qui facilite l'intégration dynamique des consommateurs au sein des processus de production, de vente et de distribution[65].

Donc, au sein des intérêts organisationnels capitalistes de Google, la surveillance des données est un moyen d'accumulation primitive – plus précisément, d'accumulation par duplication – du capital informationnel produit par les usagers[66]. Le principe de présence en amont, vu précédemment, signifie qu'en produisant du contenu et en interagissant avec les services sociotechniques et publicitaires de Google, les usagers travaillent indirectement pour l'entreprise. L'accroissement du nombre d'usagers – et la croissance du volume d'information que possède Google sur ceux-ci – avance les intérêts de sa stratégie commerciale de marchandisation des sosies de données. Au vu de sa position techno-économique inégalée, Google peut être considéré comme une superpuissance en matière de surveillance économique des données et de production

[60] Carr, Nicholas, *The Big Switch : Rewiring the World, from Edison to Google*, 121.
[61] Tene, Omer, « What Google Knows : Privacy and Internet Search Engines », *Utah Law Review*, 2008, 1451.
[62] Hansell, Saul, « Google Wants to Dominate Madison Avenue, Too », *The New York Times*, 30 octobre 2005, URL : www.nytimes.com/2005/10/30/business/yourmoney/google-wants-to-dominate-madison-avenue-too.html?_r=0 (consulté le 11 mars 2017).
[63] Tene, Omer, « What Google Knows : Privacy and Internet Search Engines », 1451.
[64] Carr, Nicholas, *The Big Switch : Rewiring the World, from Edison to Google*, 206.
[65] Elmer, Greg, *Profiling Machines : Mapping the Personal Information Economy*, The MIT Press, 2004, 8.
[66] Harvey, David, « The ''New Imperialism'' : Accumulation by Dispossession », *Actuel Marx*, vol. 1, n. 35, 2004, 71-90.

de valeur à partir des activités quotidiennes de ses usagers[67].

2.5.3. Développement d'un espace informatique général et intégré

Outre ses stratégies techniques et commerciales, Google emploie également la surveillance des données dans le cadre d'une stratégie médiatique. Conformément à son modèle d'affaires basé sur la gestion d'une économie de l'attention[68], Google tire profit de l'avantage structurel de son moteur de recherche pour s'étendre à d'autres secteurs numériques de premier plan. Cette visée coïncide avec le rôle croissant de l'Internet en tant qu'ordinateur collectif, où le stockage et le traitement de données s'apparentent à des services publics analogues au réseau électrique[69] :

> Le réseau – l'Internet – est devenu, littéralement, notre ordinateur. Les différentes composantes qui étaient auparavant isolées dans la boîte fermée de l'ordinateur – le disque dur pour entreposer l'information, le processeur pour traiter l'information, les applications pour manipuler l'information – peuvent maintenant être dispersées à travers le monde, intégrées à travers l'Internet, et partagées par tout le monde[70].

En ce sens, les ressources informatiques en 2017 sont dispersées au sein d'un réseau de données, de logiciels et d'appareils, où les technologies informatiques (téléphones cellulaires, les consoles de jeux vidéo, les ordinateurs personnels, les tablettes et autres systèmes, etc.) assument la fonction de nodule au sein d'un vaste réseau informatique[71]. C'est dans cet environnement sociotechnique caractérisé par l'infonuagique, l'interopérabilité et les « logiciels en tant que services[72] » que Google cherche à étendre ses activités pour capter et conserver l'attention des usagers.

À cette fin, Google développe et diffuse des outils conçus pour être utilisés par les usagers dans leurs activités quotidiennes. *Gmail* et *Google Hangouts* facilitent la communication entre usagers, *Google Calendar* facilite l'organisation du quotidien individuel, *Google Docs* et *Google Keep* encouragent la productivité collaborative et individuelle, *Google Play Music* et *Google*

---

[67] Fuchs, Christian, *Social Media : A Critical Introduction*, 131.
[68] Ciampaglia, Giovanni, Alessandro Flammini et Filippo Menczer, « The Production of Information in the Attention Economy », *Scientific Reports*, vol. 5, n. 9452, 2015, URL : https://www.nature.com/articles/srep09452 (consulté le 2 juin 2017).
[69] Bunker, Guy et Darren Thomson, *Delivering Utility Computing : Business-driven IT Optimization*, Wiley, 2006, 39.
[70] Carr, Nicholas, *The Big Switch : Rewiring the World, from Edison to Google*, 113-114.
[71] Carr, Nicholas, *The Big Switch : Rewiring the World, from Edison to Google*, 113-114.
[72] Armbrust, Michael *et al.*, *Above the Clouds : A Berkeley View of Cloud Computing*, University of California at Berkeley, 10 février 2009, URL : http://home.cse.ust.hk/~weiwa/teaching/Fall15-COMP6611B/reading_list/AboveTheClouds.pdf (consulté le 13 mars 2017).

Drive permettent de transférer et d'accéder à des fichiers sur un serveur infonuagique, *Google+* encourage la socialisation et le réseautage numériques, *YouTube* rassemble les créateurs et consommateurs de contenu audiovisuel, *Google Sites* facilite la création de sites web personnels et commerciaux, etc. Cet échantillon représente plusieurs dizaines de services et produits conçus pour attirer et conserver les visiteurs au sein d'un espace informationnel opérant sous la propriété de Google[73]. Comme les données personnelles peuvent être recoupées et agrégées à travers les différents services qui les produisent, la suite de produits et services de Google constitue une écologie médiatique partiellement intégrée qui se trouve renforcée par l'incursion de l'entreprise au niveau du matériel informatique, dont les ordinateurs *Chromebook* et les téléphones *Android*.

Manifestement, la prééminence incontestée de Google au niveau de son moteur de recherche et de sa position publicitaire lui permet d'investir l'ensemble des formes d'activités sociotechniques populaires. Il en résulte un monopole inégalé dans la sphère économique au niveau de l'étendue des données captées par la pléthore d'outils de Google. Cette métaposition serait nourrie par trois facteurs principaux[74]. D'abord, l'intangibilité des services numériques, contrairement par exemple aux télécommunications, réduit l'impression du risque que pose une telle prééminence au pluralisme commercial, à l'innovation et aux intérêts des consommateurs. Ensuite, la prédominance de Google se renforce elle-même, puisqu'un plus grand nombre d'usagers accroît son capital informationnel, améliore l'efficience de ses services et généralise leur utilité. Finalement, les innovations radicales développées ou acquises par Google, comme *Google Maps* et *Google Earth*, n'ont pas encore été rattrapées par les cadres législatifs et normatifs, qui favorisent pour l'instant l'autorégulation des entreprises en matière de vie privée[75].

2.6. Interprétation théorique : le métapositionnement et l'exploitation intellectuelle

La structure de pouvoir de Google réside dans le rapport organique entre l'utilisation d'un service par un usager et la création de valeur pour l'entreprise ; même les non-usagers de ses services accroissent indirectement la valeur d'usage de *Google Search* en mettant de l'information en ligne. Cette réalité est à la base du pouvoir structurel de Google. À l'inverse des organisations

[73] Girard, Bernard, *The Google Way : How One Company is Revolutionizing Management as We Know It*, 39.
[74] The Guardian, « Google dominates search. But the real problem is its monopoly on data ».
[75] Reidenberg, Joel et Thomas Davenport, « Should the U.S. Adopt European-Style Data-Privacy Protections ? », *The Wall Street Journal*, 10 mars 2013, URL : https://www.wsj.com/articles/SB10001424127887324338604578328393797127094 (consulté le 14 mars 2017).

médiatiques de contrôle de l'offre comme les journaux et les chaînes télévisées, dont le contrôle est fondé sur le filtrage et la sélection des contenus à diffuser, Google axe sa stratégie médiatique sur l'inclusion et l'accès à tout contenu à l'intérieur d'un cadre logiciel propriétaire et régi par ses conditions d'utilisation. En d'autres mots, plutôt que de déterminer quel contenu sera accessible aux individus, Google affiche tout contenu disponible sur l'Internet public, mais au sein d'un espace technique finement réglé. Cette distinction est à priori favorable aux usagers, dans la mesure où ceux-ci jouissent d'une grande liberté dans la communication, la production et l'accès au contenu. En se concentrant sur les outils communicationnels plutôt que le contenu, Google encourage et stimule la production populaire de contenu et discours, c'est-à-dire que l'entreprise laisse aux usagers la responsabilité de moduler les flux de désirs et de croyances et de mobiliser « la mémoire et l'attention qui les font circuler dans la coopération entre les cerveaux[76] ». En outre, Google conçoit et fournit des plateformes communicationnelles qui facilitent l'utilisation « des réseaux hertziens, audiovisuels, télématiques[77] » qui influencent l'opinion publique, la perception et l'intelligence collective[78].

Toutefois, cette incitation à la communication et à l'influence culturelle n'est pas désintéressée. Toute activité personnelle et sociale des usagers avance simultanément les intérêts de Google, puisqu'elle produit de l'information personnelle augmentant la valeur commerciale des produits publicitaires de l'entreprise. La gestion capitaliste des plateformes et services de Google signifie que ces derniers incorporent et opérationnalisent *d'abord* les stratégies d'accumulation de l'organisation. L'exercice d'une politique organisationnelle qui *précède* et *infléchit* les formes communicationnelles et relationnelles accessibles au public est constitutif du pouvoir structurel de l'entreprise[79]. Celui-ci repose principalement sur l'arrimage de la croissance techno-économique de l'organisation à la croissance naturelle de l'information et des usagers sur Internet.

En outre, l'hégémonie de Google est dérivée de la consubstantialité entre le médium – *Google Search*, *Google Maps* et *YouTube* – et le message – la consultation des pages des sites web publics, la cartographie routière et la production, diffusion et consommation sociales de

[76] Lazzarato, Mauricio, *Les révolutions du capitalisme*, Seuil, 2004, 83.
[77] Technologies qui combinent les télécommunications à l'informatique, comme les « téléphones intelligents ».
[78] Lazzarato, Mauricio, *Les révolutions du capitalisme*, 83.
[79] Gehl, Robert, « What's on your mind ? Social media monopolies and noopower », *First Monday*, vol. 18, n. 3, 2013, URL : http://firstmonday.org/article/view/4618/3421 (consulté le 13 février 2017)

documents audiovisuels. Ayant été en mesure de susciter un des plus importants effets de réseau tôt dans le développement commercial du web, Google est parvenu à s'étendre à différents secteurs stratégiques de la socialité numérique. À partir de cette métaposition, qui génère une valeur privée à partir de l'information produite par les usagers du web public, Google organise une partie non négligeable de la production intellectuelle et culturelle numérique. La régulation informelle qu'exercent ses algorithmes, ses interfaces et ses intérêts organisationnels structure en amont les modalités de communication, d'accès à l'information et de vie privée[80].

L'exploitation de l'intelligence collective est à la fois l'origine et la finalité des technologies de Google. Dans son ensemble, la suite de services de Google simplifie et incite des activités sociotechniques à l'intérieur d'un cadre informatique conçu pour rendre ces activités quantifiables, comparables et productives pour l'entreprise[81]. Ces services, destinés à exploiter directement et indirectement l'intelligence collective du web, sont eux-mêmes créés à partir du savoir technique et créatif des concepteurs, mathématiciens et informaticiens employés par Google.

Donc, il y a lieu de considérer la surveillance des données de Google comme une forme d'exploitation intellectuelle basée sur le pouvoir structurel : son effet de réseau lui permet d'englober une masse critique d'activité numérique sociale et personnelle au sein de ses technologies d'accumulation. Le projet d'« organiser l'information du monde » implique l'exercice d'un pouvoir structurel : un contrôle exercé *sur* l'information – par les algorithmes qui en déterminent la visibilité – et *dérivé* de l'information – par la commercialisation des données personnelles et l'exploitation du contenu public du web[82].

Cet état de fait signifie qu'il est justifié de considérer Google comme un acteur politico-économique de premier plan sur la Toile : l'entreprise est centrale à l'expérience de centaines de millions d'usagers qui, en générant des données personnelles par l'utilisation de ses services, reconduisent sa prédominance sociale, culturelle, technique et économique. Le fait que la surveillance des données soit l'axiome d'interaction central de l'entreprise signifie que l'asymétrie informationnelle est déterminante dans ses possibilités d'influence et de contrôle. La

[80] Gehl, Robert, « Knowledge Management Systems and Remote Control : Noopower and the Contemporary Transnational Corporation », dans Robert MacDougall, *Communication and Control*, Lexington Books, 2015, 10.
[81] Gehl, Robert, « What's on your mind ? Social media monopolies and noopower ».
[82] The Guardian, « Google dominates search. But the real problem is its monopoly on data ».

forme inédite de ce pouvoir technologique, arrimé à la croissance du nombre d'usagers et de l'information sur la Toile publique, confirme la nécessité d'appréhender l'importance politique du capital informationnel dans le contexte de popularisation du cyberespace.

L'importance du capital informationnel ne se limite pas à la surveillance capitaliste, puisque les agences de renseignement – en particulier la NSA et les « cinq yeux » – tentent de « tout collecter ». Bien que l'impulsion de collecte généralisée soit commune, il reste à voir, à travers une seconde étude de cas, quelles sont les cibles, principes, fonctions et objectifs de la surveillance sécuritaire des données.

Chapitre 3 : Étude de cas des pratiques de surveillance des données de la NSA

Au chapitre précédent, nous avons sommairement décrit les pratiques de surveillance des données de l'entreprise Google, ainsi que le contexte du capitalisme informationnel et les dynamiques de l'effet de réseau. En procédant d'une manière analogue, nous voulons décrire le cas de la surveillance des données conduite par la NSA en s'intéressant à ses cibles, ses principes, ses fonctions et ses objectifs. Bien entendu, les informations disponibles sont moins complètes que dans le cas de Google, étant donné le secret qui enveloppe toujours l'agence de renseignement en dépit des fuites massives de l'été 2013[1]. Conséquemment, s'il est possible et pertinent de dresser un portrait de la surveillance des données de la NSA, il demeure impossible de tout savoir à propos des programmes et des ambitions de l'agence ; seule la pointe de l'iceberg qui a été médiatisée est accessible à la recherche. L'information disponible constitue une image figée des programmes de surveillance tels qu'ils étaient en 2013 – les statistiques, modalités et opérations relatives aux programmes ont vraisemblablement changé en partie depuis. Néanmoins, l'intérêt de décrire et analyser ces programmes demeure : il est question d'identifier le contexte, les cibles, les principes, les fonctions et les buts de la surveillance des données personnelles pratiquée par la NSA, ce qui était empiriquement impossible avant 2013.

3.1. Intersection des activités des individus et des pratiques de surveillance des données de la NSA

L'intersection des activités personnelles et sociales dans le cyberespace et des pratiques de surveillance de la NSA est très large, étant donné que l'agence opère au niveau des signaux électromagnétiques dans leur ensemble. En ce sens, toute communication téléphonique, radio, satellite et numérique est susceptible d'être collectée, puis effacée ou conservée selon l'intérêt de l'information interceptée au regard des différents programmes, objectifs et autorités légales de l'agence. Deux facteurs interreliés peuvent être considérés centraux au projet de surveillance massive des données personnelles à l'échelle globale : d'un côté, l'État de sécurité nationale et son influence sur le déterminisme technomilitaire ; de l'autre, l'essor de la cybersocialité et sa

[1] En juin 2013, Edward Snowden, un employé de l'entreprise Booz Allen Hamilton contractée par la NSA, a partagé avec des journalistes du *Washington Post* et *The Guardian* des milliers de documents relatifs aux programmes et activités de surveillance de la NSA et des agences de renseignement des « cinq yeux ». Cette fuite massive a initié des réformes et des débats au niveau national et international sur la vie privée et la surveillance du cyberespace.

conceptualisation gouvernementale en tant que « nouvelle frontière[2] » à réguler et défendre.

3.1.1. La NSA et l'État de sécurité nationale américain

Lors de son allocution du 1er novembre 2013, où il défendait la pertinence des programmes de surveillance de masse de la NSA, le secrétaire d'État John Kerry (2013-2017) reconnaissait l'influence de l'État de sécurité nationale sur le développement des programmes de surveillance de masse de la NSA.

D'abord, Kerry affirma que les pratiques de la NSA reflétaient non seulement la logique de mobilisation totale de la Seconde Guerre mondiale, mais aussi le jusqu'au-boutisme justifié par la sécurité nationale dans l'endiguement communiste, puis dans la guerre contre « l'extrémisme radical[3] ». En effet, les nouvelles institutions de sécurité créées par le *National Security Act* de 1947 – qui unifiait aussi la structure du département de la Défense – constituent ce que Stuart Douglas nomme l'« État de sécurité nationale », c'est-à-dire la subordination civile des sphères politique, économique et culturelle aux questions de sécurité nationale[4]. Cette subordination continuait d'être un fait politique au moment des fuites sur la NSA en 2013, puisque la sécurité nationale était le paradigme d'interprétation dominant à partir duquel justifier l'approche préventive et intensive de la NSA : l'ancien directeur de la NSA (2000-2015), Keith Alexander, minimisa la pertinence des inquiétudes civiles soulevées par les fuites en soulignant que les programmes de surveillance étaient « extrêmement précieux [pour] protéger notre nation et assurer la sécurité de nos alliés[5] ».

Ensuite, Kerry a reconnu que le récent développement d'une surveillance de masse des données personnelles, après la surveillance ciblée des agents d'États étrangers pratiquée au 20e siècle, était tributaire d'une dynamique de « pilote automatique[6] » - en d'autres mots, d'un déterminisme issu d'une certaine constance dans les ambitions géopolitiques américaines depuis la Seconde Guerre mondiale. La politique d'endiguement du communisme avait donné lieu à la mise en

[2] Barnes, Julian, « NATO Recognizes Cyberspace as New Frontier in Defense », *The Wall Street Journal*, 14 juin 2016, URL : https://www.wsj.com/articles/nato-to-recognize-cyberspace-as-new-frontier-in-defense-1465908566 (consulté le 31 juillet 2017).
[3] Kerry, John, « Kerry : Some of NSA's 'Actions 'reached Too Far' », *YouTube*, 1 novembre 2013, URL : www.youtube.com/watch?v=hWIdYFog464 (consulté le 21 juillet 2017).
[4] Stuart, T. Douglas, *Creating the National Security State: A History of the Law that Transformed America*, Princeton University Press, 2009, 3.
[5] Boulanger, Philippe, *Géopolitique des médias : Acteurs, Rivalités et Conflits*, 97.
[6] Kerry, John, « Kerry : Some of NSA's 'Actions 'reached Too Far' ».

place d'une infrastructure planétaire destinée à l'interception des signaux électroniques centrée sur le renseignement interétatique face au bloc de l'Est et certains États[7]. Or, les budgets, les équipements et les mandats existants furent adaptés aux défis posés par la lutte au terrorisme et l'investissement massif du réseau Internet par les populations. En ce sens, les propos de Kerry font écho au rôle du phénomène de « dépendance au sentier emprunté[8] » dans l'innovation technomilitaire en général et dans le développement des programmes de surveillance de la NSA en particulier : selon lui, les programmes révélés en 2013 se sont développés de manière presque automatique « parce que la technologie est disponible, la capacité est présente, depuis une longue période de temps, remontant en fait à la Seconde Guerre mondiale[9] ». L'influence déterministe vient du fait que, dans la logique propre à l'État de sécurité nationale, « le simple fait qu'elle [la NSA] ait la capacité de collecter ces communications est devenu un justificatif pour le faire[10] ».

Cette dimension illustre la mobilisation du savoir technoscientifique aux fins du pouvoir politique, une dynamique explicitement encouragée par le *National Security Act*, qui appelle à des « efforts guidés pour réformer les procédures de collecte et de partage de renseignement, coordonner les activités des conseillers militaires et civils, et mobiliser les ressources scientifiques et économiques de la nation au nom de la préparation[11] ». Bien sûr, la conceptualisation stratégique de l'Internet en tant que vecteur militaro-politique n'est pas étrangère à l'importance des programmes de surveillance des données de la NSA[12].

En somme, le développement d'un complexe militaro-industriel – justifié par l'affrontement idéologique entre les deux superpuissances du 20e siècle et l'adaptation aux menaces asymétriques du 21e – est un facteur majeur de la prépondérance socioculturelle, économique et politique de la sécurité nationale, laquelle constitue l'axiome de la NSA dans son rapport au

[7] Gallagher, Sean, « Building a panopticon : The evolution of the NSA's XKeyscore », *Ars Technica*, 9 août 2013, URL : http://arstechnica.com/information-technology/2013/08/building-a-panopticon-the-evolution-of-the-nsas-xkeyscore/ (consulté le 5 décembre 2017).
[8] Palier, Bruno, « *Path dependence* (Dépendance au chemin emprunté) », dans Boussaquet, Laurie *et al.*, *Dictionnaire des politiques publiques*, Presses de Sciences Po, 2010, 411.
[9] Kerry, John, « Kerry : Some of NSA's 'Actions 'reached Too Far' ».
[10] Greenwald, Glenn, *No Place to Hide*, Random House, 2014, 95.
[11] Stuart, T. Douglas, *Creating the National Security State: A History of the Law that Transformed America*, 3.
[12] Joubert, Vincent, « De l'importance stratégique du cyberespace », *Analyse stratégique*, 9 novembre 2010, URL : https://dandurand.uqam.ca/wp-content/uploads/sites/3/2016/04/Joubert_cyberespace091110.pdf (consulté le 8 juin 2017).

champ global des télécommunications[13].

3.1.2. Cybersocialité et économie politique des données personnelles

Le département de la Défense des États-Unis définit le cyberespace comme un domaine caractérisé par l'usage de l'électronique et du spectre électromagnétique pour stocker, modifier et échanger des données au moyen de systèmes en réseaux et des structures physiques qui y sont attachées[14]. Cette conception a l'avantage de reconnaître que la production, la circulation et la consommation de données sont intrinsèques et centrales aux technologies numériques et réticulaires. C'est ce fait élémentaire – que les données représentent la « voie d'échappement[15] » des technologies numériques – qui sous-tend la rationalité instrumentale des programmes de surveillance de la NSA.

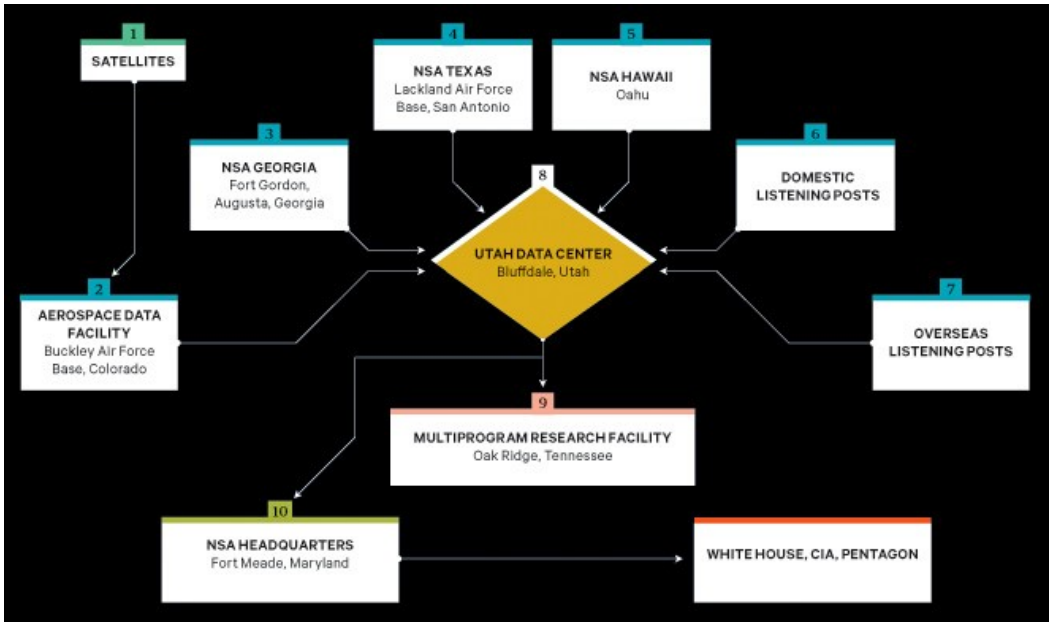
Or, l'expansion phénoménale de la cybersocialité, en particulier avec le développement du « Web 2.0. » et des médias sociaux, coïncide avec la croissance considérable du rôle, des ressources et de la marge de manœuvre de la NSA. Entre 2001 et 2013, le nombre d'employés de l'agence a crû d'un tiers pour atteindre 33 000, son budget a doublé et le nombre de compagnies privées contractées est passé de 150 à 500[16].

À cet égard, la NSA a complété en 2013 la construction d'un centre de données situé en Utah – au coût de 1,4 milliard $ US – ayant le potentiel de stocker 20 téraoctets de données par minute, soit un volume d'information équivalent à la bibliothèque du Congrès[17]. Ce centre, le quatrième plus grand dans le monde[18], sert de point de convergence des données collectées par les nombreuses installations intérieures et étrangères de la NSA.

---

[13] Friedersdorf, Conor, « Why Does Anyone Trust the National-Security State ? », *The Atlantic*, 13 novembre 2013, URL : http://www.theatlantic.com/politics/archive/2013/11/why-does-anyone-trust-the-national-security-state/281429/ (consulté le 5 décembre 2017).
[14] Samaan, Jean-Loup, « Mythes et réalités des cyberguerres », *Politique étrangère*, n. 4, hiver 2008, 829.
[15] Schneier, Bruce, *Data & Goliath – The Hidden Battles to Collect Your Data and Control Your World*, 13.
[16] Priest, Dana, « NSA growth fueled by need to target terrorists », *The Guardian*, 21 juillet 2013, URL : https://www.washingtonpost.com/world/national-security/nsa-growth-fueled-by-need-to-target-terrorists/2013/07/21/24c93cf4-f0b1-11e2-bed3-b9b6fe264871_story.html?utm_term=.7c3f62b09f83 (consulté le 13 juillet 2017).
[17] Carroll, Rory, « Welcome to Utah, the NSA's desert home for eavesdropping on America », *The Guardian*, 14 juin 2013, URL : https://www.theguardian.com/world/2013/jun/14/nsa-utah-data-facility (consulté le 9 juin 2017).
[18] Lima, Joao, « Top 10 biggest data centres from around the world », *Computer Business Review*, 2 avril 2015, URL : http://www.cbronline.com/news/data-centre/top-10-biggest-data-centres-from-around-the-world-4545356/ (consulté le 9 juin 2017).

Figure 1 – Acheminement des données entre les installations de la NSA



Source : Bamford, James, « The NSA is building the country's biggest spy center (watch what you say) », *Wired*, 15 mars 2012, URL : https://www.wired.com/2012/03/ff_nsadatacenter/ (consulté le 9 juin 2017).

Donc, le mandat institutionnel de la NSA en matière d'interception de signaux électroniques est directement concerné par les dynamiques de production, de circulation et de consommation de données qui caractérisent la cybersocialité. En d'autres mots, le processus de mise en données des relations sociales et des activités personnelles accroît la pertinence, la portée et le potentiel de l'agence de renseignement.

3.2. Les types de données personnelles collectées, traitées et analysées par la NSA

Malgré la quantité d'information rendue publique par les fuites, il est impossible de connaître tous les types de données ciblés par la NSA. Il est toutefois possible d'en dresser un portrait général à partir des programmes révélés, des propos des responsables de l'agence et des analyses de juristes et politologues. Par exemple, l'ancien directeur de la NSA, Keith Alexander, soutenait la nécessité de « tout collecter[19] », puis de trier et d'entreposer les données indéfiniment en vue de leur utilité éventuelle. Afin de « trouver l'aiguille dans la meule de foin », la technique de la

[19] Nakashima, Ellen et Joby Warrick, « For NSA Chief, terrorist threat drives passion to 'collect it all' », *The Guardian*, 14 juillet 2013, URL : https://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html?utm_term=.e45e1993eefd (consulté le 10 juin 2017).

NSA consiste à intercepter l'entièreté de la meule par tout moyen technique possible[20] :

> Pris dans leur entièreté, les documents de Snowden ont mené à une conclusion finalement simple : le gouvernement étasunien a construit un système ayant pour but l'élimination complète de la vie privée électronique à travers le monde. Loin d'une hyperbole, c'est le but littéral et explicitement affirmé de l'État de surveillance : collecter, entreposer, contrôler et analyser toutes les communications électroniques de toutes les populations autour du globe. L'agence se voue à une mission générale : empêcher que la moindre pièce d'information électronique n'échappe à sa poigne systémique[21].

En principe, aucun type de communication électromagnétique n'est formellement exclu de la collecte par les systèmes automatisés et les opérations clandestines de la NSA – et de ses alliés des « cinq yeux » – dans le cadre de ses activités de surveillance discutées plus loin.

D'abord, la NSA cible les métadonnées et communications produites par les appareils téléphoniques cellulaires et résidentiels. La compagnie *Verizon* – et d'autres compagnies majeures du réseau cellulaire américain – était sommée de fournir quotidiennement, sur une période de trois mois continuellement renouvelée, une copie de toutes les métadonnées sur les appels locaux[22] ainsi que les appels entre les États-Unis et l'étranger[23]. Ensuite, la NSA collecte quotidiennement près de cinq milliards de signaux de géolocalisation cellulaire à travers le monde, qui sont entreposés dans une base de données traquant les déplacements de centaines de millions d'appareils cellulaires[24].

Ensuite, la NSA cible les communications sur Internet de diverses façons. Notamment, à travers son accès restreint et légal aux serveurs des grandes plateformes numériques américaines depuis

---

[20] MacAskill, Ewen et Gabriel Dance, « NSA Files : Decoded – What the revelations mean for you », *The Guardian*, 1er novembre 2013, URL : https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1 (consulté le 10 juin 2017).

[21] Greenwald, Glenn, *No Place to Hide*, 94.

[22] Greenwald, Glenn, « NSA collecting phone records of millions of Verizon customers daily », *The Guardian*, 6 juin 2013, URL : https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (consulté le 11 juin 2017).

[23] Les métadonnées sont des données sur les communications. En matière téléphonique, elles peuvent inclure le numéro de téléphone du destinateur et du destinataire, la date, le temps et la durée de l'appel, le code d'identité d'abonné mobile international (IMSI), les données de géolocalisation et l'information sur le routage de la communication

[24] Gellman, Barton et Ashkan Soltani, « NSA tracking cellphones locations worldwide, Snowden documents show », *The Guardian*, 4 décembre 2013, URL : https://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html?utm_term=.d251d6862da5 (consulté le 11 juin 2017).

2008[25], la NSA peut collecter les courriels, discussions, vidéos, photos, données enregistrées, transferts de fichiers et notifications relatives à un sélecteur[26]. La NSA est aussi en mesure de collecter et filtrer en temps réel les contenus et métadonnées circulant sur Internet sans cibler de sélecteur particulier[27]. Par exemple, entre 2001 et 2011, les métadonnées sur les courriels nationaux[28] étaient collectées en vrac par la NSA[29] : « Les responsables de la NSA croyaient qu'il n'y avait pas de limites constitutionnelles sur la collecte de métadonnées numériques, incluant des détails comme l'origine, la destination et le moment des appels et des courriels[30] ». De plus, avec l'aide de l'homologue britannique de la NSA, le *Government Communications Headquarters* (GCHQ), une partie considérable du trafic circulant par les câbles de fibre optique sous-marins est interceptée et dupliqué : cette « présence en direct sur l'Internet global[31] » filtre les communications et métadonnées concernant les pages consultées, les recherches effectuées, les courriels, les discussions, l'usage d'un réseau virtuel privé, la voix par protocole Internet (VoIP), etc[32].

---

[25] Arthur, Charles, « NSA scandal : what data is being monitored and how does it work? », *The Guardian*, 7 juin 2013, URL : https://www.theguardian.com/world/2013/jun/07/nsa-prism-records-surveillance-questions (consulté le 14 juin 2017).

[26] Un sélecteur est une cible à laquelle des informations peuvent être rattachées et qui peut prendre la forme d'une adresse courriel, d'un numéro de téléphone, d'une adresse de protocole Internet, etc. Les sélecteurs constituent les cibles concrètes de la NSA, qui peut en surveiller les communications, les métadonnées et les relations avec d'autres sélecteurs.

[27] Lee, Micah, Glenn Greenwald et Morgan Marquis-Boire, « XKEYSCORE – NSA's Google for the World's Private Communications », *The Intercept*, 1 juillet 2015, URL : https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications (consulté le 14 juin 2017).

[28] Les métadonnées relatives à Internet peuvent inclure l'heure d'envoi, les adresses courriels du destinateur et du destinataire du courriel, l'information présente dans la section « sujet » du courriel, ainsi que l'adresse de protocole Internet du destinateur, des routeurs et des serveurs ayant transmis la communication. U.S. Department of Justice, « Justice Department and NSA memos proposing broader powers for NSA to collect data », *The Guardian*, 27 juin 2013, URL : https://www.theguardian.com/world/interactive/2013/jun/27/nsa-data-collection-justice-department (consulté le 11 juin 2017).

[29] Greenwald, Glenn et Spencer Ackerman, « NSA collected US email records in bulk for more than two years under Obama », *The Guardian*, 27 juin 2013, URL : https://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama (consulté le 11 juin 2017).

[30] O'Harrow Jr., Robert et Ellen Nakashima, « President's Surveillance Program worked with private sector to collect data after Sept. 11, 2001 », *The Guardian*, 27 juin 2013, URL : https://www.washingtonpost.com/investigations/presidents-surveillance-program-worked-with-private-sector-to-collect-data-after-sept-11-2001/2013/06/27/2c7a7e74-df57-11e2-b2d4-ea6d8f477a01_story.html?utm_term=.3e03479c1581 (consulté le 26 juin 2017).

[31] Angwin, Julia *et al.*, « AT&T Helped U.S. Spy on Internet on a Vast Scale », *The New York Times*, 15 août 2015, URL : https://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html (consulté le 28 juin 2017).

[32] MacAskill, Ewen, Julian Borger, Nick Hopkins *et al.*, « GCHQ taps fibre-optic cables for secret access to world's communications », *The Guardian*, 21 juin 2013, URL : https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa (consulté le 12 juin 2017).

3.3. Principes opératoires de la surveillance des données de la NSA

Les activités de la NSA sont formellement encadrées par une pluralité d'autorités découlant des branches législatives, judiciaires et exécutives de l'État fédéral américain. L'évolution de ce dispositif statutaire, au bénéfice de l'exécutif après 2001, est un des principes d'action et de marge de manœuvre de l'agence. Un second principe est l'importance de la dynamique de « présidence impériale » en matière de renseignement et de l'immunité judiciaire invoquée par le gouvernement. Enfin, un troisième principe, central à la portée globale de la NSA, est « l'avantage du terrain à domicile », c'est-à-dire les bénéfices conférés au fonctionnement des programmes de surveillance par l'ubiquité mondiale des entreprises de télécommunications américaines.

3.3.1. Contexte juridique de la surveillance de la NSA et situation de présidence impériale

Les changements apportés au cadre juridique de la surveillance étrangère au nom de la sécurité nationale constituent un axiome majeur des développements opérationnels de la surveillance des données de la NSA. Aujourd'hui, plusieurs autorités encadrent la surveillance des données de la NSA au niveau interne : le *Foreign Intelligence Surveillance Act* (FISA), lorsque la cible de la surveillance est un citoyen américain ; le *FISA Amendments Act* (FAA), lorsque la cible est raisonnablement estimée être étrangère ou bien lorsqu'une partie de la communication est étrangère ; l'autorité sur le transit, lorsque les communications sont purement étrangères et traversent le territoire étasunien. Au-delà de ces autorités internes, l'ordre exécutif 12333 (signé en 1981 par Ronald Reagan) continue d'être l'autorité primaire gouvernant les programmes de surveillance de la NSA à l'étranger :

> Un régime juridique où les données des citoyens étasuniens sont couvertes par différents niveaux de vie privée et de protection, en fonction du fait qu'elles soient collectées à l'intérieur ou à l'extérieur des frontières étasuniennes, pouvait être sensé lorsque la plupart des communications par des citoyens étasuniens restaient à l'intérieur des États-Unis. Mais aujourd'hui, les communications étasuniennes voyagent de plus en plus à travers les frontières nationales – ou sont entreposées au-delà de celles-ci[33].

[33] Napier Tye, John, « Meet Executive order 12333 : The Reagan rule that lets the NSA spy on Americans », *The Washington Post*, 18 juillet 2014, URL : https://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html?utm_term=.e6f5e71d4aee (consulté le 28 juin 2017).

Afin de comprendre la rationalité des programmes de surveillance des données de la NSA, il importe de décrire les pièces importantes du cadre juridique qui gouverne officiellement les activités de l'agence ainsi que les changements qui lui ont été récemment apportés.

3.3.1.1. Cadre statutaire de la surveillance étrangère: du comité Church au *Freedom Act* (1975-2015)

En 1975, la commission Church[34] suggéra d'encadrer différemment la surveillance en matière criminelle et la surveillance étrangère. Cette recommandation fut suivie par le Congrès avec le passage en 1978 du FISA, qui devait assurer un contrôle judiciaire en requérant l'obtention d'un mandat pour surveiller un citoyen dans un contexte de surveillance étrangère[35]. Toutefois, les demandes faites à la *Foreign Intelligence Surveillance Court* (FISC) ont lieu *ex parte*, sans l'expression d'un avis défavorable à leur mise en place. La friction entre la volonté exécutive et l'évaluation judiciaire est extrêmement faible : en 33 ans d'existence depuis la mise en œuvre du FISA, la FISC a accepté de fournir 33 942 mandats de surveillance et en a refusé douze, ce qui situe le taux de refus à 0,03 %[36].

En 1981, l'ordre exécutif 12333 encadra les pratiques de renseignement à l'étranger et constitue depuis « l'autorité primaire[37] » qui sous-tend la majorité des activités de renseignement[38]. Keith Alexander a reconnu que la majorité des données collectées par la NSA sont « uniquement en lien avec l'autorité issue de l'ordre exécutif 12333[39] ». Or, les dispositions de l'ordre furent créées antérieurement à l'ubiquité d'Internet : « le réseau global des télécommunications n'existait pas et la collecte des communications étrangères posait peu de risque que les données des citoyens américains soient captées dans le filet[40] ». Aujourd'hui, une partie non négligeable des communications étasuniennes circule dans le reste du monde et est donc happée par

[34] Comité sénatorial constitué pour enquêter sur les opérations de surveillance du gouvernement après différents abus intérieures et étrangers, notamment ceux commis par la CIA, qui furent compilés en 1973 dans un ensemble de rapports informellement nommés les *Family Jewels* (bijoux de famille).
[35] Mort, Sébastien, « Surveillance des correspondances privées dans le cyberespace aux États-Unis », *Revue française d'études américaines*, vol. 1, n. 123, 2010, 37.
[36] Perez, Evan, « Secret Court's Oversight Gets Scrutiny », *The Wall Street Journal*, 9 juin 2013, URL : https://www.wsj.com/articles/SB10001424127887324904004578535670310514616 (consulté le 17 août 2017).
[37] Watkins, Ali, « Most of NSA's data collection authorized by order Ronald Reagan issued », *McClatchy Washington Bureau*, 21 novembre 2013, URL : http://www.mcclatchydc.com/news/nation-world/national/national-security/article24759289.html (consulté le 29 juin 2017).
[38] Fidler, David, *The Snowden Reader*, Indiana University Press, 2015, 15.
[39] Napier Tye, John, « Meet Executive order 12333 : The Reagan rule that lets the NSA spy on Americans ».
[40] Watkins, Ali, « Most of NSA's data collection authorized by order Ronald Reagan issued ».

« l'univers de collecte et de stockage des communications des personnes américaines autorisé sous l'ordre exécutif 12333[41] ». Des « procédures de minimisation[42] » existent afin de limiter l'accès et l'analyse des données incidemment collectées sur des citoyens américains. Néanmoins, de nombreuses exceptions à ces procédures complexifient la situation, dont l'indication d'un crime, l'utilisation de méthodes de cryptage, ou encore la présence de renseignement utile[43]. À cet égard, il est probant que la NSA ait décliné à plusieurs reprises de fournir au Congrès une estimation du nombre de citoyens dont les communications étaient collectées, affirmant que l'agence en était incapable[44].

En 1988, un amendement à l'ordre exécutif 12333 établissait l'« autorité sur le transit », c'est-à-dire le principe permettant l'interception des communications étrangères qui circulent par les infrastructures situées en sol américain, dont la responsabilité est réservée à l'exécutif. Le développement de l'autorité sur le transit allait influencer grandement la relation entre la NSA et les compagnies de télécommunications américaines (voir 3.2).

En 1994, le *Communications Assistance to Law Enforcement Act* (CALEA) exigeait que certains fournisseurs de télécommunications adaptent leurs infrastructures afin de permettre ou de faciliter l'interception de données par les agences gouvernementales[45]. À cet égard, plus de 500 millions $ US furent dépensés par le gouvernement fédéral pour financer la conformité avec les dispositions de CALEA[46].

En 2001, le passage du *Patriot Act* assouplit le cadre judiciaire du FISA de même que les

[41] Napier Tye, John, « Meet Executive order 12333 : The Reagan rule that lets the NSA spy on Americans ».
[42] Attorney General of the United States, *Minimization Procedures Used by the National Security Agency in connection with the production of call detail records pursuant to section 501 of the Foreign Intelligence Surveillance Act, as amended*, National Security Agency, 2015, URL : https://www.nsa.gov/about/civil-liberties/reports/assets/files/UFA_SMPs_Nov_2015.pdf (consulté le 2 août 2017).
[43] Attorney General of the United States, *Minimization Procedures Used by the National Security Agency in connection with the production of call detail records pursuant to section 501 of the Foreign Intelligence Surveillance Act, as amended*,
[44] Greenwald, Glenn et James Ball, « The top secret rules that allow NSA to use US data without a warrant », *The Guardian*, 20 juin 2013, URL : https://www.theguardian.com/world/2013/jun/20/fisa-court-nsa-without-warrant (consulté le 22 juin 2017).
[45] Legal Information Institute, *47 U.S. Code Subchapter I – Interception of Digital and Other Communications*, 2017, URL : https://www.law.cornell.edu/uscode/text/47/chapter-9/subchapter-I (consulté le 22 juin 2017).
[46] Mort, Sébastien, « Surveillance des correspondances privées dans le cyberespace aux États-Unis », 43.

restrictions séparant la surveillance criminelle et la surveillance étrangère[47]. En élargissant les possibilités de surveillance intérieure, « le *Patriot Act* a fait émerger une approche de surveillance préventive qui fait de chaque citoyen un suspect potentiel dont il faut vérifier l'innocence et non plus l'implication dans des affaires criminelles[48] ». De plus, les dispositions de la loi relaxaient les conditions d'obtention d'un mandat auprès d'un juge pour une opération de surveillance, ce qui joua en faveur de « la mainmise du pouvoir exécutif sur le pouvoir législatif au nom de la sécurité nationale[49] ».

En 2011, l'administration de Barack Obama a signé une extension de trois dispositions majeures du *Patriot Act* pour une période de quatre ans[50] : la mise sur écoute itinérante[51] (*roving wiretap*), la fouille des registres commerciaux[52] et la surveillance des « loups solitaires » non affiliés aux groupes terroristes.

En 2015, le *USA Freedom Act* a renouvelé les dispositions du *Patriot Act* jusqu'en 2019, tout en amendant la section 215 sur la fouille des registres commerciaux, mettant ainsi fin à la collecte de masse effectuée par la NSA auprès des fournisseurs téléphoniques[53].

3.3.1.2. Le « programme de surveillance du président » (2001-2007)

En 2002, un ordre exécutif signé par le président George W. Bush autorisait la NSA à conduire un programme de surveillance intérieure, nommé alternativement le « programme de surveillance des terroristes » et le « programme de surveillance du président ». L'agence a ainsi intercepté et analysé les appels téléphoniques et courriels internationaux de centaines d'individus situés aux États-Unis sans avoir obtenu de mandat. Ce programme clandestin outrepassait l'autorité légale

[47] Notamment, la collecte d'information sur une puissance étrangère passa d'objet principal de l'enquête sur un individu (*the purpose*) à un objet d'importance significative (*a significant purpose*). Mort, Sébastien, « Surveillance des correspondances privées dans le cyberespace aux États-Unis », 38.
[48] Mort, Sébastien, « Surveillance des correspondances privées dans le cyberespace aux États-Unis », 48.
[49] Mort, Sébastien, « Surveillance des correspondances privées dans le cyberespace aux États-Unis », 48.
[50] Cohen, Tom, « Obama approves extension of expiring Patriot Act provisions », *CNN*, 27 mai 2011, URL : http://www.cnn.com/2011/POLITICS/05/27/congress.patriot.act/index.html (consulté le 29 juillet 2017).
[51] Réfère à la mise sur écoute sans mandat des appareils ultérieurs d'un suspect après qu'un premier appareil ait été l'objet d'un mandat.
[52] Disposition de la section 215 du *Patriot Act* permettant au FBI, par l'entremise de la FISC, d'avoir accès aux données des registres des entreprises.
[53] Yuhas, Alan, « NSA reform : USA Freedom Act passes first surveillance reform in decade – as it happened », *The Guardian*, 2 juin 2015, URL : https://www.theguardian.com/us-news/live/2015/jun/02/senate-nsa-surveillance-usa-freedom-act-congress-live?page=with:block-556e1ba8e4b07871543bacf5#block-556e1ba8e4b07871543bacf5 (consulté le 29 juillet 2017).

de la FISC en se soustrayant secrètement à l'obtention d'un mandat[54].

En 2007, la FISC approuva une partie du programme, à savoir l'interception des communications internationales impliquant un citoyen américain, à condition qu'il y ait un motif suffisant de croire qu'une des parties prenantes agisse au compte d'une organisation terroriste ou d'une puissance étrangère hostile[55]. Après avoir été essentiellement validées, les pratiques associées au programme du président furent replacées sous l'autorité de FISA et le programme lui-même fut arrêté[56].

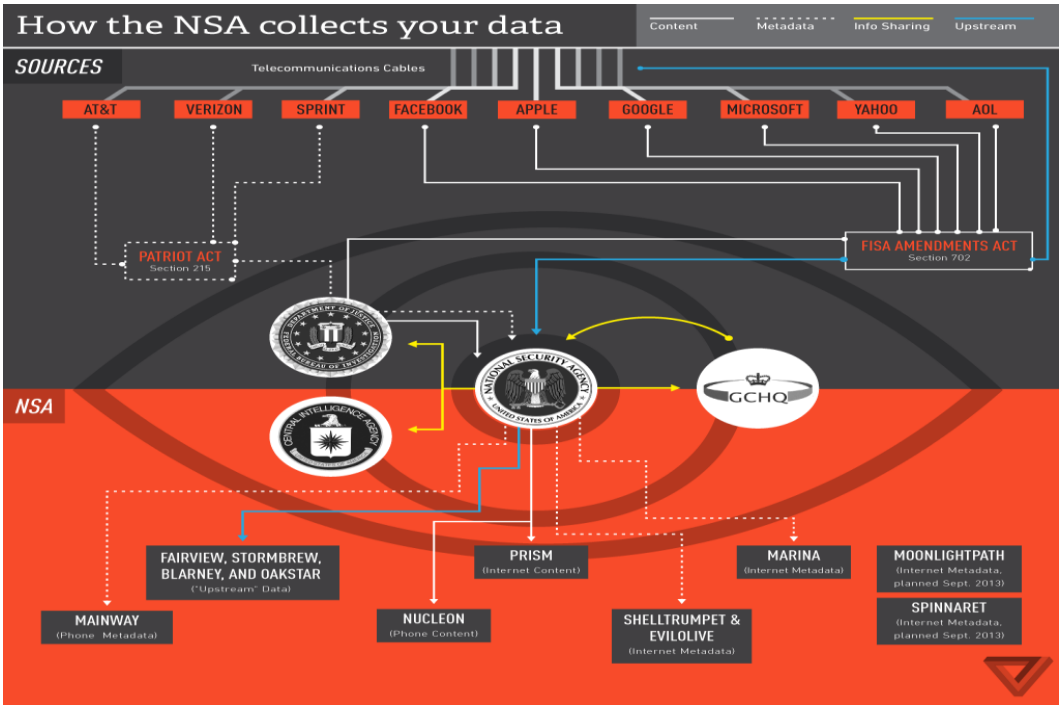
3.3.1.3. Le *FISA Amendements Act* (2008)

En 2008, la révélation de l'existence du programme clandestin mena à un vote bipartisan en faveur du FAA, qui légalisa et officialisa une dimension majeure du « programme de surveillance du président »[57]. D'une part, ce texte de loi assure rétroactivement l'immunité judiciaire aux entreprises coopérant avec la NSA ; de l'autre, il met fin au besoin d'obtenir un mandat individualisé auprès de la FISC. En effet, il n'est plus nécessaire de soumettre à la FISC la nature de l'information recherchée, l'identité de la personne et l'endroit visé par la NSA, mais seulement de confirmer que la cible de la NSA est conforme aux procédures générales approuvées annuellement par la FISC[58]. Finalement, le FAA étend les possibilités de surveillance – sans ou avant l'obtention d'un mandat – aux situations où de l'information importante à la sécurité nationale pourrait être perdue par inaction ; même si le FISC refusait d'octroyer un mandat, la NSA pourrait procéder jusqu'à ce qu'une décision finale soit prise en appel[59]. Donc, le FISA, en tant que mécanisme de contrôle judiciaire sur la surveillance des agences exécutives, doit être considéré après le FAA davantage comme un « système mettant

[54] Risen, James et Eric Lichtblau, « Bush Lets U.S. Spy on Callers Without Courts », *The New York Times*, 16 décembre 2005, URL : http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html (consulté le 27 juin 2017).
[55] Gonzales, Alberto, *Letter to Chairman Leahy and Senator Specter*, Washington D.C., The Attorney General, 17 janvier 2007, URL : http://graphics8.nytimes.com/packages/pdf/politics/20060117gonzales_Letter.pdf (consulté le 27 juin 2017).
[56] Gonzales, Alberto, *Letter to Chairman Leahy and Senator Specter*.
[57] Greenwald, Glenn, « Fisa court oversight : a look inside a secret and empty process », *The Guardian*, 19 juin 2013, URL : https://www.theguardian.com/commentisfree/2013/jun/19/fisa-court-oversight-process-secrecy (consulté le 27 juin 2017).
[58] Forgang, Jonathan, « ''The Right of the People'' : The NSA, the FISA Amendments Act of 2008, and Foreign Intelligence Surveillance of Americans Overseas », *Fordham Law Review*, vol. 78, n. 1, 2009, 238.
[59] Forgang, Jonathan, « ''The Right of the People'' : The NSA, the FISA Amendments Act of 2008, and Foreign Intelligence Surveillance of Americans Overseas », 238.

l'accent sur l'approbation efficiente des mandats basée sur la confiance en la bonne foi de l'exécutif[60] » et non sur le contrôle rigoureux de l'exécutif par le système juridique.

Figure 2 – Infographie d'une partie des relations entre la NSA, le cadre juridique et les grandes entreprises du Web et des télécommunications



Source : Sottek, T.C. et Janus Kopfstein, « Everything you need to know about PRISM », *The Verge*, 17 juillet 2013, URL : https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet (consulté le 5 juillet 2017).

3.3.2. Présidence impériale et immunité souveraine

En particulier depuis 2001, le pouvoir de l'exécutif s'est accru aux dépens de l'équilibre des pouvoirs, particulièrement en matière de surveillance et de renseignement[61]. En effet, les contestations civiles de la légalité de certaines pratiques de surveillance se heurtent d'abord à l'immunité souveraine de l'exécutif[62], puis au privilège des secrets d'État[63]. Ces deux notions

[60] Forgang, Jonathan, « ''The Right of the People'' : The NSA, the FISA Amendments Act of 2008, and Foreign Intelligence Surveillance of Americans Overseas », 239.
[61] Mody, Arjun et Corinne Curcie, *The New Imperial Presidency*, Harvard Political Review, 7 décembre 2011, URL : http://harvardpolitics.com/covers/constitution/the-new-imperial-presidency/ (consulté le 2 août 2017).
[62] L'immunité souveraine protège le gouvernement fédéral et ses agences des poursuites à moins d'une exonération exprimée dans un texte statutaire. United States District Court, « Governement Defendants' Notice of Motion to Dismiss and For Summary Judgment and Memorandum », *Jewel et al. v. National Security Agency et al.*, cas n. 08-cv-4373-VRW, 25 juin 2009, 2, URL : https://www.unitedstatescourts.org/federal/cand/207206/21-0.html (consulté le 4 décembre 2017).

furent utilisées par l'administration Bush (2001-2009) et reprises par l'administration Obama (2009-2017) afin de couper court aux poursuites relatives au dépassement allégué du cadre statutaire et constitutionnel de l'exécutif en matière de surveillance[64]. L'interprétation de l'administration Obama ne restreignait pas l'immunité souveraine aux poursuites liées au *Foreign Intelligence Surveillance Act* – comme c'était le cas de l'administration Bush[65] –, mais l'étendait aussi à celles liées au *Wiretap Act*[66] et au *Stored Communications Act*[67].

De plus, la NSA possède une marge de manœuvre considérable, sans contrôle législatif ou judiciaire, sous l'autorité de l'ordre exécutif 12333. La sénatrice Dianne Feinstein (D-CA), présidente de la Commission du Sénat sur le renseignement, a reconnu que les programmes sous l'ordre exécutif 12333 étaient « entièrement sous la branche exécutive[68] » et « insuffisamment» contrôlés par le Congrès. D'ailleurs, les fuites de Snowden ont révélé que la NSA avait comptabilisé à l'interne plus de 2 000 violations de ses standards de conformité entre 2011 et 2012 dans les programmes issus de l'ordre exécutif 12333, sans que celles-ci aient à être communiquées au comité sur le renseignement[69].

3.3.3. L'avantage du terrain à domicile

Un troisième principe majeur qui sous-tend les pratiques de surveillance des données de la NSA est l'exceptionnelle concentration sur le territoire américain des grands acteurs techniques et économiques du cyberespace. En effet, la centralité des États-Unis dans les télécommunications, le divertissement et l'innovation technologique exerce un effet centripète sur les usagers à l'échelle globale et facilite ainsi le travail des agences de renseignement : il est estimé que 90

---

[63] Privilège dispensant le gouvernement de présenter ses éléments de preuve si ceux-ci sont des secrets d'État pouvant porter atteinte à la sécurité nationale. Fisher, Louis, « State Secrets Privilege », *Library of Congress*, 2015, URL : https://www.loc.gov/law/help/usconlaw/state-privilege.php (consulté le 26 juin 2017).
[64] Edelson, Chris, *Power Without Constraint : The Post-9/11 Presidency and National Security*, Wisconsin, University of Wisconsin Press, 2016, 78.
[65] United States District Court, « Government Defendants' Notice of Motion to Dismiss and For Summary Judgment and Memorandum », 2.
[66] Loi fédérale de 1968 régulant les activités de collecte du contenu des communications privées téléphoniques et électroniques.
[67] Loi fédérale de 1986 régulant le partage volontaire et obligatoire des enregistrements des transactions et des communications téléphoniques et électroniques possédées par des tiers partis.
[68] Watkins, Ali, « Most of NSA's data collection authorized by order Ronald Reagan issued », *McClatchy Washington Bureau*, 21 novembre 2013, URL : http://www.mcclatchydc.com/news/nation-world/national/national-security/article24759289.html (consulté le 29 juin 2017).
[69] Watkins, Ali, « Most of NSA's data collection authorized by order Ronald Reagan issued ».

% des communications mondiales traversent les États-Unis d'une manière ou d'une autre[70]. Grâce à l'autorité sur le transit, dont nous avons discuté précédemment, cette centralité dans les télécommunications permet aux agences américaines de « se connecter localement pour atteindre des cibles globalement[71] ». De plus, la prééminence sociotechnique de Google, Apple, Facebook, Amazon et Microsoft (GAFAM)[72] signifie que leurs usagers internationaux soumettent leurs données personnelles à la juridiction étasunienne, facilitant dès lors le travail des agences de renseignement :

> Bien que les programmes de surveillance d'Internet de la NSA opéraient de manière extra-légale après le 11 septembre 2001, ils opèrent maintenant au sein d'une infrastructure légale qui leur permet de tirer avantage de la domination étasunienne de l'Internet. […] Avec le passage du *FISA Amendements Act* (FAA) en 2008, la FISC peut approuver la surveillance des personnes non étasuniennes hors des États-Unis sans mandat individualisé. Ces changements ont fourni la base légale pour des programmes de la NSA comme PRISM, qui implique l'obtention de données de communications à partir de compagnies d'Internet comme [GAFAM][73].

Dans ses activités de surveillance des données, la NSA peut compter sur plus de 80 « partenariats stratégiques[74] » avec de grandes multinationales américaines de télécommunications qui ont un rôle important dans l'acheminement et le routage des communications internationales : AT&T, IBM, Cisco, Motorola, Intel, Verizon, Qualcomm, Hewlett-Packard, Oracle et Microsoft sont explicitement mentionnées[75]. Ces relations contractuelles sont entretenues et gérées par une division spécifique de la NSA, les *Special Source Operations* (SSO), qui fut qualifiée par le lanceur d'alerte Edward Snowden de « bijou de la couronne[76] » de la NSA. En effet, selon un document interne de la NSA, les SSO génèrent plus de 80% de l'information collectée par les systèmes de l'agence[77]. Les documents internes définissent ces activités corporatives comme « l'accès et la collecte de télécommunications par câble, par commutateur réseau et/ou par routeur rendus possibles par les partenariats impliquant la NSA et des compagnies de

[70] Ball, James, « NSA stores metadata of millions of web users for up to a year, secret files show », *The Guardian*, 30 septembre 2013, URL : https://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents (consuté le 24 juin 2017).
[71] Ambinder, Marc, « Sources : NSA sucks in data from 50 companies », *The Week*, 6 juin 2013, URL : http://theweek.com/articles/463456/sources-nsa-sucks-data-from-50-companies (consulté le 24 juin 2017).
[72] Google, Amazon, Facebook, Apple, Microsoft.
[73] Austin, Lisa, « Lawful Illegality : What Snowden Has Taught Us about the Legal Infrastructure of the Surveillance State », chapitre dans Michael Geist et Wesley Wark, *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, Ottawa, University of Ottawa Press, 2015, 115-116.
[74] Greenwald, Glenn, *No Place to Hide*, 102.
[75] Greenwald, Glenn, *No Place to Hide*, 102.
[76] Greenwald, Glenn, *No Place to Hide*, 102.
[77] Angwin, Julia *et al.*, « AT&T Helped U.S. Spy on Internet on a Vast Scale ».

télécommunications commerciales[78] ».

Parmi ces partenariats stratégiques, la relation de la NSA avec AT&T constitue une figure d'exception. En effet, la NSA jouit d'une relation « hautement collaborative » bâtie depuis des décennies sur l'« extrême volonté d'aider » manifestée par AT&T : contrairement aux autres SSO, il est question « d'un partenariat, non pas d'une relation contractuelle[79] ». En tant que cas avancé de coopération d'une entreprise de télécommunications avec l'État de sécurité nationale, la description de la relation de la NSA avec AT&T permet de jauger l'importance de l'avantage du terrain à domicile et du concept de « nébuleuse de surveillance étatique et corporative[80] ».

La proximité entre le gouvernement fédéral et AT&T est vieille de plus d'un demi-siècle. En 1967, le président Gerald Ford intervenait politiquement afin de protéger AT&T d'une sommation à comparaître en insistant sur la position stratégique occupée par l'entreprise au regard de la sécurité nationale :

> Agissant […] sous l'autorité du président des États-Unis, l'*American Telephone and Telegraph Company* est engagée pour fournir des services essentiels à la sécurisation d'information vitale à la protection de la sécurité nationale et de la politique étrangère des États-Unis. En raison de la position unique de cette compagnie par rapport aux lignes de communications téléphoniques et autres aux États-Unis […] la branche exécutive lui a partagé de l'information sensible à la sécurité nationale[81].

Le cas de Ford présage les dispositions du FAA (2008), qui conféra l'immunité judiciaire rétroactive à AT&T dans le cadre de sa coopération avec les agences exécutives. Cette décision visait à mettre fin aux poursuites civiles entamées en 2006 par l'*Electronic Frontier Foundation* (EFF) après les révélations de Mark Klein, un technicien d'AT&T pendant plus de 20 ans ayant sonné l'alerte sur la collaboration de l'entreprise avec la NSA. Klein avait découvert que AT&T entretient depuis 2003 des « chambres secrètes » réservées à la NSA au sein d'au moins 17 de ses installations en sol américain[82]. Klein a publicisé l'existence d'une pièce située dans les bureaux de San Francisco, défendue d'accès aux techniciens d'AT&T et réservée à un spécialiste ayant

[78] National Security Agency, « Newly Disclosed N.S.A. Files Detail Partnerships With AT&T and Verizon », *The New York Times*, 15 août 2015, URL : https://www.nytimes.com/interactive/2015/08/15/us/documents.html (consulté le 29 juin 2017).
[79] Angwin, Julia *et al.*, « AT&T Helped U.S. Spy on Internet on a Vast Scale ».
[80] Coleman, Roy, « The imagined city : Power, mystification and synoptic surveillance », chapitre dans Kirstie Ball, *The Surveillance-Industrial Complex : A Political Economy of Surveillance*, Routledge, 2013, 143.
[81] Ford, Gerald, « American Telephone and Telegraph Subpoena, 6/76 (2) », *The White House*, Washington, D.C., 1976, URL : https://www.fordlibrarymuseum.gov/library/document/0014/19077243.pdf (consulté le 2 juillet 2017).
[82] Angwin, Julia *et al.*, « AT&T Helped U.S. Spy on Internet on a Vast Scale ».

une attestation de sécurité de la NSA : la « chambre 641A[83] ». Dans celle-ci, AT&T dupliquait le trafic Internet circulant dans les câbles de fibre optique de son réseau *WorldNet*, qui fait partie de l'épine dorsale d'Internet[84], vers un superordinateur, le Narus STA 6400. Le superordinateur utilise un logiciel d'analyse sémantique du trafic (STA)[85], « conçu pour fouiller rapidement à travers des grands volumes de données qui circulent à haute vitesse, en cherchant en fonction de différents algorithmes[86] ». Narus, l'entreprise à l'origine du matériel et du logiciel en question, fut fondée par d'anciens membres de l'Unité 8200 – l'homologue israélien de la NSA – avant d'être achetée par le fournisseur de la Défense américaine Boeing[87].

Au-delà de ce cas spécifique, AT&T collabore extensivement avec les projets de surveillance de la NSA. Par exemple, la multinationale a installé de l'équipement de surveillance dans au moins 59 villes américaines[88]. L'entreprise a également fourni une assistance technique à la mise sous écoute de toutes les communications Internet du bâtiment des quartiers généraux de l'Organisation des Nations-Unies (ONU) à New York, qui faisait affaire avec AT&T[89]. De plus, le plus grand centre de traitement d'appels téléphoniques interurbains dans le monde, une tour complètement dénuée de fenêtres située en plein cœur de Manhattan, appartient à AT&T ; cette tour, nommée TITANPOINTE par la NSA, est un lieu important d'analyse des communications non seulement téléphoniques et numériques, mais aussi satellites[90].

En somme, l'avantage du terrain à domicile est le résultat de la présence globale des multinationales de télécommunications américaines et de la volonté politique pour instrumentaliser cette présence à des fins stratégiques. La portée et l'intensité des capacités de

---

[83] PBS, « Spying on the Home Front : Interview – Mark Klein », *Frontline*, 15 mai 2007, URL : http://www.pbs.org/wgbh/pages/frontline/homefront/interviews/klein.html (consulté le 1er juillet 2017).
[84] L'épine dorsale d'Internet est l'ensemble physique constitué de la grille de lignes de fibre optique à haute capacité qui achemine la masse du trafic Internet, ainsi que du système de commutateurs et routeurs qui dirigent ce trafic. Mulligan, Thomas, « The Internet Backbone », *Los Angeles Times*, 3 février 1997, URL : http://articles.latimes.com/1997-02-03/business/fi-25071_1_internet-backbone (consulté le 1er juillet 2017).
[85] Wired Staff, « AT&T Whistle-blower's evidence », *Wired*, 17 mai 2006, URL : https://www.wired.com/2006/05/att-whistle-blowers-evidence/ (consulté le 1er juillet 2017).
[86] PBS, « Spying on the Home Front : Interview – Mark Klein ».
[87] Kane, Alex, « How Israel Became a Hub for Surveillance Technology », *The Intercept*, 17 octobre 2016, URL : https://theintercept.com/2016/10/17/how-israel-became-a-hub-for-surveillance-technology/ (consulté le 1er juillet 2017).
[88] Gallagher, Ryan et Henrik Moltke, « Titanpointe – The NSA's Spy Hub in New York, Hidden in Plain Sight », *The Intercept*, 16 novembre 2016, URL : https://theintercept.com/2016/11/16/the-nsas-spy-hub-in-new-york-hidden-in-plain-sight/ (consulté le 2 juillet 2017).
[89] Angwin, Julia *et al.*, « AT&T Helped U.S. Spy on Internet on a Vast Scale ».
[90] Gallagher, Ryan et Henrik Moltke, « Titanpointe – The NSA's Spy Hub in New York, Hidden in Plain Sight ».

surveillance de la NSA seraient profondément compromises sans la coopération – volontaire ou mandatée – des multinationales de télécommunications basées aux États-Unis[91], dont au premier chef AT&T.

3.4. Usages tactiques (fonctions) de la surveillance des données

Le cadre statutaire entourant les activités de surveillance étrangère et intérieure permet de constater l'existence d'une pluralité d'autorités formant une nébuleuse plus ou moins cohérente et en partie outrepassée par certains privilèges attribués à la branche exécutive. Ce corpus d'autorités contextualise la variété des programmes de surveillances à la disposition de la NSA.

La surveillance des données peut être déclinée en deux catégories de programmes, soit ceux opérant en amont (*upstream*) et ceux opérant en aval (*downstream*)[92]. Étant donné la grande variété et complexité des programmes de la NSA, nous nous limiterons à la description d'un corpus composé de quatre programmes : trois en amont et un en aval. Les programmes ont été sélectionnés en fonction de la diversité des tactiques décrites, de la représentativité des actions de la NSA et de l'accès au fonctionnement des programmes.

3.4.1. La surveillance des données en amont

La surveillance des données en amont réfère à une interception durant leur passage par les câbles sous-marins de fibre optique qui connectent l'infrastructure globale des télécommunications[93]. La surveillance en amont se divise en trois portfolios de programmes distincts : la collaboration avec les multinationales américaines de télécommunications, la collaboration avec d'autres agences de renseignement et l'interception unilatérale faite sans la connaissance du gouvernement ou de l'entreprise responsable[94]. Nous étudierons un programme de surveillance en amont issu de

---

[91] O'Harrow Jr., Robert et Ellen Nakashima, « President's Surveillance Program worked with private sector to collect data after Sept. 11, 2001 », *The Guardian*, 27 juin 2013, URL : https://www.washingtonpost.com/investigations/presidents-surveillance-program-worked-with-private-sector-to-collect-data-after-sept-11-2001/2013/06/27/2c7a7e74-df57-11e2-b2d4-ea6d8f477a01_story.html?utm_term=.3e03479c1581 (consulté le 26 juin 2017).

[92] National Security Agency, *Statement – NSA Stops Certain Section 702 ''Upstream'' Activities*, 28 avril 2017, URL : https://www.nsa.gov/news-features/press-room/statements/2017-04-28-702-statement.shtml (consulté le 3 juillet 2017).

[93] Timberg, Craig, « NSA slide shows surveillance of undersea cables », *The Washington Post*, 10 juillet 2013, URL : https://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html?utm_term=.77d0cac92628 (consulté le 3 juillet 2017).

[94] Gellman, Barton et Matt DeLong, « The NSA's three types of cable interception programs », *The Washington Post*, s/d, URL : http://apps.washingtonpost.com/g/page/world/the-nsas-three-types-of-cable-interception-programs/553/ (consulté le 3 juillet 2017).

chacun des trois portfolios : *FAIRVIEW*, *MUSCULAR* et *MYSTIC*.

3.4.1.1. FAIRVIEW

Le programme FAIRVIEW est issu du portfolio corporatif et repose entièrement sur un même partenaire corporatif ayant accès aux câbles, aux routeurs et aux commutateurs internationaux : la multinationale américaine des télécommunications AT&T. Il s'agit d'un programme majeur de surveillance des données en amont, puisqu'il serait parmi les cinq programmes les plus utiles à la surveillance continue de cibles à l'échelle globale[95]. Un document interne de la NSA souligne que le partenaire corporatif de FAIRVIEW est « agressivement impliqué dans le modelage du trafic de sorte à faire passer des signaux d'intérêts[96] » vers les systèmes de l'agence. L'infrastructure utilisée pour FAIRVIEW est entièrement intérieure et existe depuis 1985[97].

Les aspects uniques de ce programme, selon la NSA, incluent « l'accès à des quantités massives de données[98] ». En effet, dès 2003, le développement d'une « présence en direct sur Internet » permit à l'entreprise de fournir 400 milliards de métadonnées numériques à l'agence en l'espace d'un mois et plus d'un million de courriels par jour vers les systèmes d'analyse automatisés[99]. Un second aspect unique est le contrôle du programme par plusieurs autorités légales : FISA, FAA et l'autorité sur le transit. Par conséquent, les modalités de la surveillance des données varient selon les autorités légales et les types de cibles: les communications de citoyens ou d'étrangers en territoire américain requièrent un mandat individualisé de la FISA ; les communications entre les États-Unis et l'étranger doivent cadrer avec les catégories justificatives présentées annuellement à la FISC dans le cadre du FAA ; les communications purement étrangères ne nécessitent aucune approbation extérieure[100].

3.4.1.2. WINDSTOP et MUSCULAR

Ensuite, au sein du second portfolio de la surveillance des données en amont, basé sur la coopération d'agences de renseignement étrangères, le programme WINDSTOP désigne tous les

---

[95] Greenwald, Glenn, *No Place to Hide*, 104.
[96] Harcourt, Bernard, *Exposed : Desire and Disobedience in the Digital Age*, Harvard University Press, 2015, 72.
[97] Angwin, Julia *et al.*, « AT&T Helped U.S. Spy on Internet on a Vast Scale ».
[98] Greenwald, Glenn, *No Place to Hide*, 104.
[99] Angwin, Julia *et al.*, « NSA Spying Relies on AT&T's ''Extreme Willingness to Help'' », *Scientific American*, 17 août 2015, URL : https://www.scientificamerican.com/article/nsa-spying-relies-on-at-t-s-extreme-willingness-to-help/ (consulté le 20 août 2017).
[100] Angwin, Julia *et al.*, « AT&T Helped U.S. Spy on Internet on a Vast Scale ».

sous-programmes poursuivis avec d'autres membres des « cinq yeux ». Parmi ceux-ci, un sous-programme se démarque par l'implication centrale du Royaume-Uni, nommé MUSCULAR. La relation de la NSA avec le GCHQ est l'axe principal des « cinq yeux », bien que l'organisation s'assure de mobiliser les capacités de chacun au bénéfice de tous[101]. Entre 2010 et 2013, le gouvernement des États-Unis a payé près de 160 millions $US au GCHQ, notamment afin de « garantir l'accès à et l'influence sur les programmes de collecte de renseignement du Royaume-Uni[102] ». Le GCHQ, qui dépend de la NSA pour plus de 60 % de ses renseignements de haute valeur, considère important d'être vu par la NSA comme faisant sa part, notamment en mettant à profit ce que l'agence considère être les avantages du Royaume-Uni combinant « géographie, partenariats et régime juridique[103] » : le Royaume-Uni est situé dans une position névralgique parmi les réseaux de câbles sous-marins qui relient les continents ; le GCHQ peut mettre à contribution ses propres relations avec plusieurs entreprises et États étrangers ; le cadre juridique des activités de surveillance au Royaume-Uni est moins strict qu'aux États-Unis[104].

La fonction du programme MUSCULAR est de contourner le cryptage des données personnelles effectué par Google et Yahoo!! en infiltrant le réseau interne qui connecte respectivement leurs centres de données à travers le monde[105]. Comme les données circulant dans le réseau interne des deux multinationales ne sont pas cryptées, la NSA et le GCHQ obtiennent un accès à de grandes quantités d'informations personnelles :

> Intercepter des communications outre-mer a des avantages clairs pour la NSA, avec des restrictions plus souples et moins de comptes à rendre. Les documents de la NSA à propos de l'effort réfèrent directement à la 'collecte complète', à 'l'accès en vrac' et aux opérations de 'haut volume' à l'endroit des réseaux de Yahoo! et de Google. Une telle collecte à grande échelle de contenu Internet serait illégale aux États-Unis, mais les opérations ont lieu outre-mer, où la NSA a le droit de présumer que quiconque utilisant des connexions étrangères est un étranger. Hors du territoire étasunien, les restrictions statutaires sur la surveillance ne s'appliquent pas et la FISC n'a aucune

[101] Greenwald, Glenn, *No Place to Hide*, 118.
[102] Hopkins, Nick et Julian Borger, « Exclusive : NSA pays £100m in secret funding for GCHQ », *The Guardian*, 1er août 2013, URL : https://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden (consulté le 4 juillet 2017).
[103] Hopkins, Nick et Julian Borger, « Exclusive : NSA pays £100m in secret funding for GCHQ ».
[104] Leigh, Ian, « Ministers exploit legal grey area to justify GCHQ spying », *Durham University News*, 6 février 2014, URL : https://www.dur.ac.uk/news/newsitem/?itemno=20968 (consulté le 19 août 2017).
[105] Gellman, Barton et Ashkan Soltani, « NSA infiltrates links to Yahoo!, Google data centers worldwide, Snowden documents say », *The Washington Post*, 30 octobre 2013, URL : https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-Yahoo!-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html?utm_term=.b1e758ad97fc (consulté le 4 juillet 2017).

juridiction[106].

À partir de lieux d'interceptions situés hors du territoire américain, la NSA et le GCHQ dupliquent et filtrent l'entièreté des flux de données qui traversent les câbles de fibre optique reliant les nombreux centres de données des deux compagnies américaines. Le GCHQ permet à la NSA de lui soumettre jusqu'à 100 000 sélecteurs à partir desquels cibler l'information en transit[107] :

> Pour le projet MUSCULAR, le GCHQ dirige toute la collecte vers un « tampon » qui peut contenir de trois à cinq jours de trafic avant de devoir recycler l'espace de stockage. À partir du tampon, des outils conçus sur mesure par la NSA décortiquent et décodent les formats de données spéciaux que les deux entreprises [Google et Yahoo!] utilisent à l'intérieur de leurs infonuages. Ensuite, les données sont envoyées à travers une série de filtres pour 'sélectionner' l'information que la NSA veut […]. S'introduire dans les infonuages de Google et Yahoo! permet à la NSA d'intercepter des communications en temps réel et de poser 'un regard rétrospectif sur l'activité de la cible', selon un document interne de la NSA[108].

3.4.1.3. MYSTIC

Finalement, au sein du troisième portfolio, caractérisé par les activités unilatérales de la NSA, le programme MYSTIC se distingue par sa capacité de surveillance inédite. En effet, le système permet à la NSA d'enregistrer l'entièreté des appels téléphoniques d'un pays étranger, de les entreposer pendant un mois et d'ainsi « revenir dans le passé[109] » d'une cible après qu'elle ait été identifiée. Le programme a été utilisé à l'insu des cinq pays visés : le Mexique, le Kenya et les Philippines ont vu leurs métadonnées collectées par la NSA, tandis que les Bahamas et l'Afghanistan[110] furent l'objet d'une collecte complète (*full-take*) du contenu et des métadonnées

---

[106] Gellman, Barton et Ashkan Soltani, « NSA infiltrates links to Yahoo!, Google data centers worldwide, Snowden documents say ».

[107] Gellman, Barton et Ashkan Soltani, « NSA infiltrates links to Yahoo!, Google data centers worldwide, Snowden documents say ».

[108] Gellman, Barton et Ashkan Soltani, « NSA infiltrates links to Yahoo!, Google data centers worldwide, Snowden documents say ».

[109] Gellman, Barton et Ashkan Soltani, « NSA surveillance program reaches 'into the past' to retrieve, replay phone calls », *The Washington Post*, 18 mars 2014, URL : https://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html?utm_term=.b3d6d2877fa1 (consulté le 5 juillet 2017).

[110] Lors de la couverture médiatique initiale du programme MYSTIC, l'identité d'un des pays visés avait été censurée à la demande du gouvernement américain, en raison du risque que la révélation posait aux opérations en cours dans le pays. Après que l'organisation de transparence *Wikileaks* ait révélé qu'il s'agissait de l'Afghanistan, seul le média *Russia Today* a couvert la nouvelle. Russia Today, *'Country X' : WikiLeaks reveals NSA recording*

des appels. Bien que peu d'information ait été publiée sur le fonctionnement du programme, « un mémo indique que […] les données sont clandestinement acquises sous les auspices des ''interceptions légitimes'' conduites au moyen des ''accès'' de la *Drug Enforcement Administration* – des mises sur écoute licites des réseaux téléphoniques étrangers que la DEA peut demander dans le cadre de la coopération internationale en matière policière[111] ». L'infrastructure de MYSTIC peut traiter quotidiennement plus de 100 millions d'appels[112]. Le programme atteste de l'efficience technologique et de l'emprise géopolitique de la NSA : la capacité de collecter l'entièreté des communications téléphoniques d'un pays ciblé est d'une valeur stratégique considérable.

3.4.2. La surveillance des données en aval : PRISM

Les programmes décrits précédemment opèrent en amont en interceptant les flux de communications durant leur transit. Le second grand versant des activités de surveillance de la NSA procède en aval : par un accès légal et limité aux bases de données corporatives, par un accès clandestin et illimité dérivé de l'exploitation des vulnérabilités informatiques des services commerciaux[113] et par l'installation de logiciels-espions, faite à distance ou en détournant des livraisons de matériel informatique[114].

Le programme de surveillance des données en aval le plus médiatisé par les fuites d'Edward Snowden est indéniablement le programme PRISM, notamment parce qu'il implique les plus importantes entreprises du Web et la continuation de certaines pratiques de surveillance initiées par le « programme de surveillance du président » (2001-2007)[115]. Le programme PRISM exploite le modèle d'affaires des grandes corporations de l'Internet, fondé sur la

---

'nearly all' phone calls in Afghanistan, 24 mai 2014, URL : https://www.rt.com/news/160988-wikileaks-nsa-phone-afghanistan/ (consulté le 5 juillet 2017).

[111] Devereaux, Ryan, Glenn Greenwald et Laura Poitras, « Data pirates of the Caribbean », *The Intercept*, 19 mai 2014, URL : https://theintercept.com/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/ (consulté le 5 juillet 2017).

[112] Devereaux, Ryan, Glenn Greenwald et Laura Poitras, « Data pirates of the Caribbean ».

[113] Reynaud, Florian, « Le business des ''zero day'', ces failles inconnues des fabricants de logiciel », *Le Monde*, 23 septembre 2015, URL : http://www.lemonde.fr/pixels/article/2015/09/23/le-business-des-zero-day-ces-failles-inconnues-des-fabricants-de-logiciel_4768638_4408996.html (consulté le 1 août 2017).

[114] Spiegel Staff, « Inside TAO : Documents Reveal Top NSA Hacking Unit – Part 3 : The NSA's Shadow Network », *Spiegel Online*, 29 décembre 2013, URL : http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969-3.html (consulté le 1 août 2017).

[115] Sottek, T.C. et Janus Kopfstein, « Everything you need to know about PRISM », *The Verge*, 17 juillet 2013, URL : https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet (consulté le 5 juillet 2017).

commercialisation des données personnelles, en accédant aux données et métadonnées personnelles des usagers des entreprises ou services suivants : Microsoft, Yahoo!, Google, Facebook, PalTalk, AOL, Skype, YouTube et Apple. Le programme n'implique pas de mandat individuel auprès de la FISC pour les usagers estimés d'être à l'extérieur des États-Unis, seulement la garantie que les cibles surveillées sont conformes aux lignes directrices approuvées annuellement en vertu du FAA[116].

Le programme de surveillance fonctionne par le biais d'une interface gérée par le FBI, où la NSA peut formuler des requêtes de données et de métadonnées qui sont acheminées aux différentes compagnies[117] :

> La demande de recherche, appelée '*tasking*', peut être envoyée à de multiples sources. Un *tasking* pour Google, Yahoo!, Microsoft, Apple et d'autres fournisseurs passe par un équipement installé à chaque compagnie. Cet équipement, géré par le FBI, communique la requête de la NSA au système d'une compagnie privée. Selon la compagnie, un *tasking* peut fournir des courriels, des pièces jointes, des carnets d'adresses, des calendriers, des fichiers entreposés dans l'infonuage, du clavardage texte, audio ou vidéo, et des « métadonnées » qui identifient le lieu, les appareils utilisés et d'autres informations à propos d'une cible[118].

Nonobstant les coûts encourus par la NSA pour adapter les systèmes informatiques des entreprises concernées, estimés à plusieurs millions de dollars, l'agence considère PRISM comme « un des accès les plus utiles, uniques, et productifs[119] ». Vers la fin de l'année 2012, PRISM collectait les données personnelles rattachées à au moins 45 000 sélecteurs[120].

---

[116] Gellman, Barton et Todd Lindeman, « Inner workings of a top-secret spy program », *The Washington Post*, 29 juin 2013, URL : https://www.washingtonpost.com/apps/g/page/national/inner-workings-of-a-top-secret-spy-program/282/ (consulté le 3 juillet 2017).

[117] Gellman, Barton et Laura Poitras, « U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program », *The Washington Post*, 6 juin 2013, URL : https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_print.html (consulté le 5 juillet 2017).

[118] Gellman, Barton et Todd Lindeman, « Inner workings of a top-secret spy program », *The Washington Post*, 29 juin 2013, URL : https://www.washingtonpost.com/apps/g/page/national/inner-workings-of-a-top-secret-spy-program/282/ (consulté le 3 juillet 2017).

[119] Hopkins, Nick, « UK gathering secret intelligence via covert NSA operation », *The Guardian*, 7 juin 2013, URL : https://www.theguardian.com/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism (consulté le 6 juillet 2017).

[120] Follorou, Jacques et Glenn Greenwald, « France in the NSA's crosshair : Wanadoo and Alcatel targeted », *Le Monde*, 21 octobre 2013, URL : http://www.lemonde.fr/technologies/article/2013/10/21/france-in-the-nsa-s-crosshair-wanadoo-and-alcatel-targeted_3499739_651865.html (consulté le 6 juillet 2017).

Figure 3 – Tableau issu de la NSA comparant la surveillance en aval (PRISM) et en amont

Opérations sous FAA-702. Pourquoi faut-il utiliser à la fois PRISM et la surveillance en amont.		
	PRISM [surveillance en aval]	**Surveillance en amont**
Surveillance d'Internet	9 fournisseurs de services basés aux É-U	Sources à travers le monde
Surveillance téléphonique	Non ; à venir bientôt.	Sources à travers le monde
Accès aux communications entreposées (recherche)	Oui	Non
Collecte en temps réel	Oui	Oui
Collecte basée sur des mots-clés	Non	Oui
Collecte de la voix	Oui	Oui
Relation directe avec les fournisseurs de communications	Non ; seulement par l'entremise du FBI.	Oui

Source : Diapositive interne de la NSA. The Guardian, *NSA Prism program slides*, 1 novembre 2013, 4, URL : https://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document (consulté le 3 août 2017).

Le tableau ci-dessus explique que PRISM devait, en 2013, bientôt permettre de cibler des sélecteurs téléphoniques, qu'il ne permettait pas de cibler des communications à partir de mots-clés, que la relation avec les entreprises était gérée par le FBI, que le programme permettait à la NSA d'accéder aux données antérieures au début du suivi d'un sélecteur. Autrement dit, une fois qu'une cible est désignée, PRISM rend possible la collecte des communications antérieures : un avantage important de la surveillance en aval sur la surveillance en amont.

3.5. Usages stratégiques (buts) de la surveillance des données de la NSA

Manifestement, la variété et l'intensité des programmes de surveillance de la NSA – dont

seulement quatre ont été décrits sur plus d'une quinzaine – sont autant de tactiques imbriquées au sein de stratégies politiques communes à l'agence, au système gouvernemental américain ainsi qu'à l'alliance non institutionnalisée des « cinq yeux ». Nous concevons la notion de stratégie comme la poursuite d'un plan reliant plusieurs fins entre elles par adaptation dynamique qui soit intimement liée à l'acquisition d'information :

> Le mot stratégie ne désigne pas un programme prédéterminé qu'il suffit d'appliquer […]. La stratégie permet, à partir d'une décision initiale, d'envisager un certain nombre de scénarios pour l'action, scénarios qui pourront être modifiés selon les informations qui vont arriver en cours d'action et selon les aléas qui vont survenir […]. La stratégie profite du hasard et, quand il s'agit de la stratégie à l'égard d'un autre joueur, la bonne stratégie utilise les erreurs de l'adversaire. […] La construction du jeu se fait dans la déconstruction du jeu adverse. […] La stratégie lutte contre le hasard et cherche l'information. […] Le hasard n'est pas seulement le facteur négatif à réduire dans le domaine de la stratégie. C'est aussi la chance à saisir[121].

Cette conception cybernétique de la stratégie est bien adaptée aux systèmes de surveillance de la NSA, où le hasard représente une vulnérabilité qu'il est impératif de minimiser chez soi et d'exploiter pleinement chez les adversaires. En ce sens, la notion de stratégie dans le cyberespace partage certains aspects avec la doctrine de supériorité informationnelle du département de la Défense abordée plus loin[122].

La surveillance des données personnelles conduite par la NSA sert au moins trois objectifs généraux : la production de renseignements opérationnels pour d'autres institutions gouvernementales, la défense des systèmes informatiques critiques à la sécurité nationale et l'établissement et le maintien de la suprématie informationnelle de l'État fédéral américain.

3.5.1. Produire des renseignements opérationnels pour d'autres institutions gouvernementales

Le rôle central de la NSA est de produire des renseignements opérationnels pour une multitude d'institutions gouvernementales des États-Unis. Le métapositionnement de la NSA en matière informationnelle représente un apex à partir duquel générer des savoirs tactiques utiles aux branches militaires, économiques et diplomatiques du gouvernement fédéral, qui dépendent

[121] Morin, Edgar, *Introduction à la pensée complexe*, Éditions du Seuil, 2005, 106.
[122] Department of Defense, *Strategy for Operations in the Information Environment*, juin 2016, URL : https://www.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf (consulté le 11 juillet 2017).

d'une connaissance optimale de l'environnement informationnel globalisé. À cet égard, la NSA coopère, entre autres, avec le département d'État, le département de l'Agriculture, le département du Trésor, le département du Commerce et le département de l'Énergie et s'assure qu'ils reçoivent « le renseignement critique et les produits et services d'assurance informatique dont ils ont besoin pour accomplir leurs missions et protéger la nation[123] ».

Figure 4 – Tableau issu de la NSA répertoriant ses consommateurs de renseignement

Classification des consommateurs du renseignement produit par la NSA		
Producteurs majeurs de renseignement complet	**Décideurs et forces de l'ordre**	**Secteur militaire et tactique**

• Agence du renseignement de la défense (DIA)
• Agence nationale de renseignement géospatial (NGA)
• Bureau du renseignement et de la recherche (INR)
• CIA
• Conseil national du renseignement
	• Ambassadeurs des É-U
	• Congrès
	• Directeur du renseignement central (DCI)
	• Départements de :
	  • l'Agriculture
	  • de la Justice
	  • du Trésor
	  • du Commerce
	  • de l'Énergie
	  • d'État
	  • de la Sécurité intérieure
	• Maison-Blanche
	• Représentants commerciaux des É-U
		• Alliances
		• Chef de l'état-major interarmées
		• Commandants en chef
		• Commandements tactiques
		• Département de la Défense
		• Forces de l'ONU
		• Forces opérationnelles
		• OTAN

Source : Greenwald, Glenn, *No Place to Hide*, p. 136.

Toutefois, la position informationnelle centrale occupée par la NSA au sein du système institutionnel de l'État fédéral américain signifie que ses programmes de surveillance remplissent des fonctions allant bien au-delà de l'identification des menaces et de la défense des systèmes informatiques critiques. En effet, la NSA sert les intérêts de l'État américain non seulement en identifiant et en surveillant les menaces asymétriques et informatiques, mais aussi en versant dans la surveillance économique, commerciale, diplomatique et politique de certains États,

[123] National Security Agency, *Customers & Partners*, 27 mai 2016, URL : https://www.nsa.gov/what-we-do/customers-and-partners/ (consulté le 7 juillet 2017).

entreprises, acteurs et institutions régionales et internationales[124].

En ce sens, la NSA a pour fonction stratégique de convertir la fongibilité des ressources informationnelles qu'elle acquiert en un vaste éventail de renseignements qui offrent des avantages tactiques à l'État américain sur la scène internationale. La valeur ajoutée produite par les programmes de la NSA élève la position informationnelle du gouvernement des États-Unis par rapport aux autres acteurs du système international. Par exemple, lors du cinquième Sommet des Amériques s'étant déroulé à Trinité-et-Tobago en avril 2009, plus de 100 rapports générés par la NSA permirent au département d'État d'utiliser à son avantage une « profonde connaissance des plans et intentions des autres participants[125] ». La NSA remplit une fonction cruciale pour une panoplie de stratégies gouvernementales qui dépendent de l'information :

> Détenir l'information et être capable de s'en servir le premier, c'est la promesse d'une supériorité sur tout partenaire ou adversaire : supériorité immédiate et de peu de temps, mais qui peut devenir une supériorité irréversible, si la détention d'une première information est à son tour capable d'en générer d'autres, ou d'induire à la conquête suivie d'une série ininterrompue d'informations nouvelles, toujours un peu « en avance » sur l'évènement ou sur l'adversaire[126].

3.5.2. Défendre les systèmes informatiques critiques et agir contre les menaces

La NSA a également pour objectif stratégique de défendre les systèmes informatiques jugés comme étant critiques pour la sécurité nationale. En conformité avec ce mandat, la NSA défend les États-Unis – incluant leurs intérêts et leurs alliés – des terroristes, des cybercriminels, des pirates informatiques et des gouvernements étrangers hostiles en surveillant les données relatives au trafic illégal des drogues, à la prolifération des armes de destruction massive et aux attaques informatiques[127].

L'objectif défensif de l'agence se décline en deux aspects tactiques complémentaires : « comprendre qui sont nos adversaires, où ils sont situés et quels sont leurs capacités, plans et

---

[124] Watts, Jonathan, « NSA accused of spying on Brazilian oil company Petrobras », *The Guardian*, 9 septembre 2013, URL : https://www.theguardian.com/world/2013/sep/09/nsa-spying-brazil-oil-petrobras (consulté le 12 juillet 2018).
[125] Greenwald, Glenn, *No Place to Hide*, 139.
[126] Varet, Gilbert, *Pour une science de l'information comme discipline rigoureuse*, Paris, Les Belles Lettres, 1987, 38.
[127] National Security Agency, *Understanding the Threat*, 3 mai 2016, URL : https://www.nsa.gov/what-we-do/understanding-the-threat/ (consulté le 9 juillet 2017).

intentions[128] », d'un côté, tout en protégeant les informations et systèmes de la sécurité nationale américaine, de l'autre. En ce sens, la vigilance à l'endroit des « menaces à la sécurité nationale très réelles et très graves[129] » signifie, d'abord, une pluralité d'efforts visant à « tromper, bloquer, perturber, détériorer et détruire[130] » certaines informations et certains systèmes d'informations à travers le monde, et ensuite, l'identification des menaces potentielles grâce à des technologies de classification des individus et de leurs données selon une échelle du risque.

En raison de la structure complexe du cyberespace, le rôle de protection des systèmes informatiques critiques rapproche inévitablement la NSA des grandes entreprises américaines de télécommunications qui, par leurs activités multinationales, assument des responsabilités communicationnelles critiques. L'importance axiomatique de l'innovation privée à la suprématie technologique des États-Unis brouille la distinction entre les installations publiques et privées en matière de sécurité nationale, notamment dans le contexte de la compétitivité internationale en recherche et développement. La protection des informations sensibles à la sécurité nationale implique une défense de la propriété intellectuelle, qui structure l'innovation technologique[131]. À cet égard, la NSA soutient la nécessité d'intégrer les grands acteurs informationnels du secteur privé aux initiatives gouvernementales en matière de sécurité nationale et économique :

> Pour maintenir leur avantage concurrentiel dans le marché mondial, les compagnies ont besoin de protéger agressivement leur propriété intellectuelle de tous les types d'activités et de techniques d'exploitation utilisées pour l'acquérir et l'utiliser illégalement. Cette protection doit venir de solutions innovantes créées par l'accroissement des partenariats et des programmes gouvernementaux et commerciaux alignés pour protéger l'information commerciale sensible et la propriété intellectuelle. Autrement, notre avantage économique compétitif dans l'économie globale, atteint à travers l'innovation, la créativité et l'intégrité de notre peuple, est menacé[132].

Donc, la surveillance des données de la NSA sert à maintenir un statu quo non seulement politique et militaire, mais aussi technoscientifique et économique : la situation de prééminence étasunienne où les intérêts gouvernementaux et ceux des grands acteurs privés convergent.

---

[128] National Security Agency, *Understanding the Threat*.
[129] National Security Agency, *Understanding the Threat*.
[130] Joint Chiefs of Staff, *Cyberspace Operations*, 5 février 2013, II-5, URL : http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf (consulté le 19 août 2017).
[131] Kalanje, M. Christopher, « Role of Intellectual Property in Innovation and New Product Development », *World Intellectual Property Organization*, s/d, URL : http://www.wipo.int/sme/en/documents/ip_innovation_development_fulltext.html (consulté le 19 août 2017).
[132] National Security Agency, *Cyber*, 19 juillet 2017, URL : https://www.nsa.gov/what-we-do/cyber/ (consulté le 19 juillet 2017).

3.5.3. Établir, soutenir et accroître la suprématie informationnelle de l'État fédéral étasunien

L'augmentation continue du rôle et des ressources de la NSA depuis 2001 est directement tributaire de l'importance croissante du renseignement électromagnétique, notamment pour la communauté du renseignement, les unités militaires et le FBI[133]. Même en 2000, soit avant l'essor récent de la NSA, l'agence était à l'origine de 60 % de l'information présente dans le breffage quotidien du président[134]. Selon l'agence, « les signaux étrangers que la NSA collecte sont inestimables pour la sécurité nationale », puisqu'ils aident à « déterminer où nos adversaires sont situés, ce qu'ils planifient, le moment où ils prévoient agir, avec qui ils travaillent, et les types d'armes qu'ils utilisent[135] ».

L'utilité première de la NSA au sein de l'État fédéral réside en sa capacité à défendre les systèmes informatiques critiques contre les cyberattaques et à produire des renseignements opérationnels sur des cibles militaires, politiques, diplomatiques et économiques. Cette fonction duelle signifie que la pertinence de la NSA croît proportionnellement à l'importance et à l'ubiquité d'Internet et des TIC. L'agence occupe une position névralgique pour la doctrine technomilitaire de supériorité informationnelle et sa finalité, la « suprématie dans tous les domaines » (*full-spectrum dominance*) : terre, mer, air, espace et *information*[136].

Ce dernier domaine, l'environnement informationnel, est défini par le département de la Défense comme un agrégat composé de l'information ainsi que des individus, des organisations et des systèmes qui la collectent, la traitent ou la disséminent[137]. Un document projetant les stratégies militaires américaines à l'horizon 2020 affirme que l'environnement informationnel doit être investi de part en part afin de générer et de soutenir la supériorité informationnelle : la capacité de collecter, de traiter et de disséminer un flux ininterrompu d'informations tout en privant ou en

[133] Priest, Dana, « NSA growth fueled by need to target terrorists », *The Guardian*, 21 juillet 2013, URL : https://www.washingtonpost.com/world/national-security/nsa-growth-fueled-by-need-to-target-terrorists/2013/07/21/24c93cf4-f0b1-11e2-bed3-b9b6fe264871_story.html?utm_term=.7c3f62b09f83 (consulté le 13 juillet 2017).
[134] Priest, Dana, « NSA growth fueled by need to target terrorists ».
[135] Priest, Dana, « NSA growth fueled by need to target terrorists ».
[136] Institute for National Strategic Studies, *Joint Vision 2020. America's Military – Preparing for Tomorrow*, U.S. Government Printing Office, 2000, 61, URL : http://www.dtic.mil/dtic/tr/fulltext/u2/a526044.pdf (consulté le 17 juillet 2017).
[137] Institute for National Strategic Studies, *Joint Vision 2020. America's Military – Preparing for Tomorrow*, 62.

minimisant cette capacité chez l'adversaire[138]. Le maintien de la supériorité informationnelle dépend du succès des opérations informationnelles, c'est-à-dire les actions prises pour affecter l'information et les systèmes d'information d'un adversaire tout en défendant sa propre information et ses propres systèmes d'information[139]. Le département de la Défense anticipe que les opérations dans l'environnement informationnel deviendront à terme aussi importantes stratégiquement et opérationnellement que celles conduites sur terre, sur mer, dans l'air et dans l'espace[140] :

> Le mot supériorité implique un état ou une condition de débalancement en sa propre faveur. La supériorité informationnelle est de nature transitoire et doit être créée et soutenue par les forces armées conjointes à travers la conduite d'opérations informationnelles. Toutefois, le développement d'une supériorité informationnelle n'est pas une fin en soi. La supériorité informationnelle fournit à la force conjointe un avantage compétitif seulement lorsqu'elle est effectivement traduite en connaissances et en décisions supérieures[141].

La surveillance des données personnelles à l'échelle globale est un aspect fondamental des opérations informationnelles. En ce sens, la variété des programmes de la NSA cadre avec les variables des opérations informationnelles : la signification multidimensionnelle de l'information, qui peut être une cible, une arme, une ressource ou un domaine ; les différents niveaux d'action – tactique, opérationnel ou stratégique ; la nature de la situation (temps de paix, de crise ou de conflit) ; les objectifs des opérations, comme fournir de l'information, gérer les perceptions, dominer un champ de bataille, opérer une guerre du commandement et du contrôle, perturber ou détruire des systèmes[142]. Les programmes de surveillance des données de la NSA sont structurés par les variables des opérations informationnelles et guidés par la doctrine de suprématie informationnelle : la NSA est l'agence la mieux placée pour dominer l'environnement informationnel, c'est-à-dire « tout savoir sur l'adversaire en l'empêchant d'en savoir beaucoup sur soi[143] ».

En somme, les programmes et le pouvoir technique de la NSA doivent être situés dans le contexte de reproduction et de sécurisation de la supériorité informationnelle de l'État américain

---

[138] Institute for National Strategic Studies, *Joint Vision 2020. America's Military – Preparing for Tomorrow*, 62.
[139] Institute for National Strategic Studies, *Joint Vision 2020. America's Military – Preparing for Tomorrow*, 72.
[140] Institute for National Strategic Studies, *Joint Vision 2020. America's Military – Preparing for Tomorrow*, 72.
[141] Institute for National Strategic Studies, *Joint Vision 2020. America's Military – Preparing for Tomorrow*, 62.
[142] Institute for National Strategic Studies, *Joint Vision 2020. America's Military – Preparing for Tomorrow*, 72.
[143] Arquilla, John, « The Strategic Implications of Information Dominance », *Strategic Review*, vol. 22, n. 3, 1994, 25.

par le biais d'opérations informationnelles, dont la surveillance des données est partie intégrante. En effet, la surveillance en amont et en aval de l'Internet, tout comme l'idéal de « tout collecter » prisé par Keith Alexander, s'inscrit dans la stratégie de suprématie informationnelle en développant « la capacité à accéder à plus d'information et à de l'information plus complète plus rapidement que les adversaires à courts et longs termes[144] ».

3.6. Interprétation théorique : la NSA comme produit et reproducteur du lien gouvernemental entre le savoir et le pouvoir

Au sein du système gouvernemental des États-Unis et du réseau anglo-saxon des « cinq yeux », la NSA assume une position prédominante dans la production de renseignements utiles (*actionable intelligence*) à une pluralité de stratégies géopolitiques. La surveillance des données conduite par la NSA a connu une expansion significative avec le déclenchement de la « guerre au terrorisme » en 2001, ce qui coïncide avec la popularisation d'Internet et le développement d'une cybersocialité ubiquitaire. La régulation informelle des potentialités subversives du nouveau médium de masse va au-delà de la lutte antiterroriste et s'inscrit dans une stratégie étatique de contrôle social basée sur la lisibilité des populations[145].

> Suite aux développements politiques depuis le 11-Septembre (de même que des développements juridiques et économiques durant les années 1990), le discours de la puissance s'est concentré sur l'établissement d'une suprématie informationnelle dans tous les domaines, le déclenchement de frappes informationnelles préventives ainsi que sur une rhétorique insistant sur le système particulièrement ouvert et anarchique de l'Internet en tant que danger plutôt qu'opportunité. L'information est décrite comme un outil ou une arme plutôt que comme un bien collectif, alors que l'Internet peut être utilisé comme un multiplicateur de force pour générer des effets sur des populations cibles[146].

La contribution de l'agence à la position prédominante des États-Unis dans le système international illustre la relation réciproque entre le pouvoir et le savoir. D'un côté, la concentration inouïe du capital technologique et humain de la NSA repose sur la suprématie des États-Unis en matière militaire et technoscientifique ; de l'autre, la NSA mobilise ses capacités technologiques pour générer des savoirs exploitables par l'État américain au service du maintien

[144] McEvoy Manjikian, Mary, « From Global Village to Virtual Battlespaces : The Colonizing of the Internet and the Extension of Realpolitik », 386-387.
[145] Scott, C. James, *Seeing Like A State : How Certain Schemes to Improve the Human Condition Have Failed*, 183.
[146] McEvoy Manjikian, Mary, « From Global Village to Virtual Battlespaces : The Colonizing of the Internet and the Extension of Realpolitik », 386-387.

de sa « suprématie dans tous les domaines » :

> L'information est une connaissance […] moins acquise par les moyens de la connaissance (raisonnement, observation, expérience) que par les moyens mêmes de la puissance : réseau d'infiltration territoriale, jeux de stratagèmes et de prévision aléatoire, usage d'armes de guerre, d'engins sophistiqués ou d'argent. […] Une propriété très sensible de l'information à ce stade, c'est son caractère fusible, fongible, périssable : l'information se consomme; et elle se consume définitivement avec l'exécution à laquelle elle donne lieu[147].

Le cyberespace est activement conceptualisé par le département de la Défense comme l'un de ces réseaux d'infiltration territoriale, où une technologie communicationnelle perturbatrice[148] s'impose comme un médium universel ultimement instrumentalisé par les « engins sophistiqués » de la NSA afin de générer des connaissances utiles, contingentes et fongibles[149], qui constituent pour les décideurs du système gouvernemental étasunien un avantage reposant sur l'asymétrie de savoir en leur faveur[150]. L'étude des pratiques de surveillance de la NSA permet de voir à l'œuvre la réciprocité entre le savoir et le pouvoir, où l'innovation scientifique et technologique altère continuellement l'environnement et les possibilités stratégiques[151].

[147] Varet, Gilbert, *Pour une science de l'information comme discipline rigoureuse*, 39.
[148] National Research Council, *Persistent Forecasting of Disruptive Technologies*, The National Academies Press, 2010, 40.
[149] Par exemple, une même information concernant les communications d'un ambassadeur étranger peut servir les intérêts de différents départements du gouvernement fédéral étasunien, notamment le département d'État, le département du Commerce ou encore le département de la Défense.
[150] Lightfoot, Geoffrey et Tomasz Wisniwski, *Information Asymmetry and Power in a Surveillance Society*, MPRA, 2014, 23, URL : https://mpra.ub.uni-muenchen.de/58726/8/MPRA_paper_58726.pdf (consulté le 2 août 2017).
[151] Rappert, Brian, *Technology and Security : Governing Threats in the New Millenium*, Springer, 2007, 29.

Chapitre 4: Comparaison analytique des pratiques de surveillance des données de Google et de la NSA

Au cours des deux chapitres précédents, nous avons décrit les contextes, les cibles, les principes, les fonctions et les objectifs de la surveillance des données personnelles conduite par deux organisations majeures du cyberespace, soit Google et la NSA. La comparaison entre les dynamiques de la surveillance des données chez une agence de renseignement et chez une entreprise privée est informée par un concept important de la littérature sur la surveillance contemporaine, celui de « nébuleuse de surveillance étatique et corporative » : une situation de convergence entre les intérêts, les technologies et les pratiques d'États et de grandes entreprises multinationales en faveur de la diffusion et de la normalisation de la surveillance individualisée des populations. L'analyse comparée des deux organisations choisies permet de contribuer empiriquement au champ sociopolitique couvert par ce concept.

Dans ce chapitre, ces deux entités sont comparées entre elles en tenant compte de la position dominante qu'elles occupent dans leur champ d'action respectif en matière de collecte, de stockage, d'analyse et d'exploitation des données personnelles. Le chapitre analytique vise à identifier les dynamiques aussi bien divergentes que convergentes en se basant sur les descriptions effectuées dans les deux études de cas. Par le biais de cette perspective comparée, nous comptons ensuite formuler certaines observations d'ordre général et théorique sur la complémentarité de la surveillance commerciale et de la surveillance sécuritaire des données personnelles. Après l'analyse des résultats, il sera possible d'effectuer un retour sur la littérature ainsi que sur la validité interne et la validité externe de notre étude, tout en soulignant certaines pistes de recherche pertinentes. La conclusion sera l'occasion de poser un regard sur l'ambiguïté politique d'Internet entre les perturbations populaires et les stratégies des États industriels avancés et de l'innovation entrepreneuriale.

4.1. Comparaison des contextes systémiques de Google et de la NSA

Les deux études de cas ont permis de constater que la surveillance des données repose sur la conjonction de phénomènes antécédents, dont l'innovation technique et économique ainsi qu'un changement dans les attitudes et comportements sociotechniques populaires. Les facteurs systémiques communs apparaissent alors comme un point de départ pertinent pour une

perspective comparée sur les organisations informationnelles que sont Google et la NSA. Il est possible de noter au moins trois facteurs systémiques qui sous-tendent leur prédominance de Google et de la NSA : la *position* dominante des États-Unis, le *terrain* sociotechnique des données personnelles et la *structure* ouverte, universelle et circulatoire d'Internet.

Au premier plan, les deux organisations sont conditionnées par la structure unipolaire du système international en matière technologique et militaire. La prévalence du capital intellectuel, technologique et organisationnel des États-Unis depuis la Seconde Guerre mondiale constitue un facteur systémique qui sous-tend la prééminence des deux organisations dans leurs champs respectifs. À cet égard, l'invention du réseau Internet issue de la collaboration des milieux scientifiques et militaires étasuniens atteste du positionnement avantageux des organisations nationales dans son exploitation. Google et la NSA constituent des figures prééminentes de l'utilisation stratégique du cyberespace à des fins respectivement commerciales et sécuritaires, mais qui contribuent toutes deux aux intérêts nationaux des États-Unis. Donc, la centralité politique, technique, économique et militaire des États-Unis dans le système international est un facteur systémique du degré de sophistication et de marge de manœuvre des deux organisations.

Au deuxième plan, le contrôle qu'exercent Google et la NSA dans leurs domaines respectifs dépend de l'adoption préalable, massive et profonde des TIC par les populations. L'importance systémique des deux organisations augmente de pair avec la croissance de l'usage des TIC et d'Internet : l'accumulation d'un capital informationnel utile est dépendante du fait qu'une masse critique d'individus normalisent la mise en données de leurs communications personnelles et des détails de leur vie privée. Si Google et la NSA fonctionnent tous les deux selon un modèle centralisé soutenu par une rationalité cybernétique, il demeure néanmoins que le phénomène de surveillance des données s'appréhende « du bas vers le haut » : la mise en données des vies individuelles constitue *d'abord* un terrain sociotechnique, sur lequel se déploient *ensuite* diverses stratégies organisationnelles relatives au captage, au traitement, à l'organisation et à l'exploitation des données personnelles. La croissance significative de la lisibilité du social par la mise en données des quotidiens, des activités, des préférences et des communications constitue un changement systémique propice à l'essor de la surveillance de masse des données personnelles, autant dans le modèle d'affaires de Google que dans les pratiques de la NSA.

Au troisième plan, le fonctionnement et les activités des deux organisations sont conditionnés par les structures d'Internet. Le réseau est global, public et fonctionne par un échange constant de données et de métadonnées entre les serveurs (les ordinateurs qui assurent le fonctionnement d'un site web) et les clients (les ordinateurs utilisés par les usagers). Or, la combinaison de ces caractéristiques crée un terrain fertile pour le développement et l'ascendance d'organisations spécialisées dans la collecte de données: le caractère global en fait un marché sans frontières ; le caractère public élimine presque tout coût à l'acquisition de l'information ; l'échange constant de données normalise la circulation automatisée des informations des usagers et fait de toute action individuelle une *communication* destinée à une ou plusieurs machines. Avant la commercialisation et la généralisation d'Internet, aucune compagnie privée n'était en mesure de posséder tant d'information sur autant de dimensions de la vie des consommateurs, tandis que le mandat de la NSA était alors restreint au renseignement interétatique. En somme, le modèle d'affaires de Google et la réorientation des activités de la NSA ont été conditionnés par les possibilités offertes par les structures sociotechniques d'Internet.

4.2. Comparaison des types de données ciblées par Google et la NSA

Sans procéder à une comparaison de chacun des types de données que collectent respectivement les deux organisations, il est possible d'affirmer à partir des études de cas que l'étendue des types de données est considérablement plus vaste dans le cas de la NSA que dans celui de Google. Cette différence est liée aux finalités distinctes qui orientent les deux types de surveillance des données.

En effet, Google a intérêt à ne collecter seulement que les données personnelles étant utiles d'un point de vue commercial ou technique. Les données personnelles récoltées par l'entreprise sont utiles au niveau technique – à l'exécution d'un programme, à la personnalisation d'un service, à la création d'un compte ou encore à la vérification de l'identité – ou bien au niveau commercial – au raffinement des algorithmes et à la bonification des produits publicitaires. En ce sens, Google n'a pas d'intérêt organisationnel envers la collecte de données extérieures à son champ d'activité, bien que celui-ci soit large, ce qui fonde l'autolimitation rationnelle et intéressée de ses processus de surveillance. Dans un marché hautement compétitif et rationalisé, la surveillance des données obéit à la même évaluation des coûts et des bénéfices que les activités économiques classiques.

Quant à la NSA, celle-ci n'est pas soumise à la même contrainte utilitaire, étant donné la nature de son mandat et l'origine exogène de ses ressources. Comme la sécurisation du champ des télécommunications n'est possible que par une application systématique et globale des appareils de surveillance, la collecte des données de la NSA se distingue de la rationalité économique de Google en captant des volumes faramineux de données souvent triviales. Les types de données surveillées par la NSA n'ont théoriquement aucune limite, étant donné que la surveillance des données obéit à un impératif sécuritaire qui ne saurait exclure d'emblée une quelconque forme d'information personnelle. La surveillance sécuritaire des signaux électroniques, pour être effective dans la détection et l'identification des différentes menaces, doit nécessairement s'étendre à toute la sphère des communications informatiques et satellites : c'est ce qui sous-tend la formule du « *collect it all, process it all, exploit it all*[1] » prisée par les responsables de la NSA depuis 2001. En ce sens, la grande majorité des données collectées par la NSA est à priori dénuée d'une quelconque valeur commerciale, politique, sécuritaire ou stratégique.

Donc, d'un côté, le processus de surveillance des données personnelles de Google discrimine en faveur d'un corpus restreint de types de données utilitaires et productifs destiné à être exploité en profondeur ; de l'autre, le processus de surveillance des données de la NSA s'applique de manière indiscriminée à un ensemble indéfini de communications et de signaux électroniques, dont la majorité est à priori inutile. Il faut préciser que ce constat a pour exception les programmes de surveillance de la NSA qui ciblent expressément des personnalités politiques, criminelles ou militaires précises, où l'exploitation des données collectées est plus approfondie que dans le cas de Google. Néanmoins, dans le cadre de l'objet de recherche – la surveillance *de masse* des données personnelles – la distinction faite entre Google et la NSA s'applique.

4.3. Comparaison des principes de fonctionnement

Les principes commerciaux ou sécuritaires qui sous-tendent le fonctionnement de la surveillance des données exercent une influence sur les types de données collectées, sur les façons dont elles sont obtenues et exploitées ainsi que sur les finalités qu'elles servent. Il s'agit d'un axe majeur de différenciation des pratiques de surveillance des données : alors que Google opère selon une rationalité économique et des intérêts commerciaux, la NSA opère selon une rationalité

[1] The Intercept. *Elegant Chaos : collect it all, exploit it all (plus notes)*, 6 septembre 2016, URL : https://theintercept.com/document/2016/09/06/elegant-chaos-collect-it-all-exploit-it-all-plus-notes/ (consulté le 23 octobre 2017).

gouvernementale et des intérêts sécuritaires. En somme, les processus de surveillance des données sont infléchis par les distinctions organisationnelles entre une entreprise privée et une agence de renseignement.

4.3.1. De la rationalité commerciale à la rationalité sécuritaire

En ce qui concerne Google, cet infléchissement par la rationalité économique se traduit non seulement par l'autolimitation en matière de collecte, mais aussi par la nécessité légale d'obtenir le consentement des individus auprès desquels s'effectue la surveillance. Ce consentement prend la forme de l'acquiescement aux conditions d'utilisation qui établissent la propriété de l'entreprise sur les données produites durant l'utilisation de ses services et logiciels. Comme l'acquiescement à ce contrat est l'unique barrière à l'utilisation, il fait office de compensation par l'utilisateur en échange de la gratuité et de l'efficience des services de Google. De plus, la collecte est justifiée par la garantie que les informations collectées améliorent et personnalisent les services de Google, ce qui profite directement et indirectement aux usagers.

En ce qui concerne la NSA, la rationalité gouvernementale et le cadre juridique dispensent l'agence d'obtenir le consentement des individus étant l'objet des programmes de surveillance des données, bien qu'elle implique également des limitations statutaires qui proscrivent formellement certaines catégories d'individus pouvant en faire l'objet, dont au premier chef les citoyens étasuniens. Néanmoins, comme l'a souligné l'étude de cas sur la NSA, les privilèges accordés aux agences exécutives, dont l'immunité judiciaire et le droit d'exception, permettent de contourner ces limitations dans certaines situations. De plus, la dispersion mondiale des communications nationales rend inévitable la collecte de communications de citoyens étasuniens, bien que celles-ci soient ensuite traitées selon des protocoles distincts. Hormis le cas des nationaux, la NSA n'est aucunement restreinte dans ses activités de surveillance qui sont pour la plupart gouvernées par l'ordre exécutif 12333.

> L'ordre exécutif 12333 ne contient rien qui empêche la NSA de collecter et d'entreposer […] le contenu et les métadonnées – pourvu que ladite collecte ait lieu à l'extérieur des États-Unis dans le cadre d'une enquête de renseignement étranger qui soit légale. Aucun mandat et aucun accord d'une cour de justice ne sont requis, et la collecte n'a pas besoin d'être rapportée au Congrès[2].

[2] Napier Tye, John, « Meet Executive order 12333: The Reagan rule that lets the NSA spy on Americans.

En tant qu'agence exécutive, la NSA bénéficie de l'autorité régalienne dérivée de la présidence. Contrairement à Google, dont les activités doivent répondre – au moins en partie – aux attentes des actionnaires, la NSA est plus imperméable aux volontés extérieures à sa chaîne de commandement restreinte. Elle est plus libre que l'entreprise de procéder de manière ad hoc et expérimentale de manière souvent temporairement, comme de nouveaux programmes, l'exploitation de nouvelles failles informatiques, le développement de nouveaux logiciels ou le début d'une coopération avec une entreprise ou une agences de renseignement étrangère. La NSA procède selon ses besoins organisationnels tels qu'ils sont librement interprétés à partir de ses mandats en matière de défense des systèmes critiques et de production de renseignement.

4.3.2. Entreprise privée et agence exécutive: responsabilité et autonomie

Les deux organisations ont en commun d'être hautement centralisées et en grande partie automatisées. Il est possible de dresser un parallèle entre la logique cybernétique des technologies informatiques, une structure « de commandement et de contrôle » (*command and control*) qui relaie les décisions du centre aux unités du réseau, et la structure élitiste des deux organisations.

Dans le cas de la NSA, la décision quant aux orientations de l'organisation dépend du directeur national du renseignement, du directeur de la NSA, du secrétaire de la Défense et, ultimement, de la présidence. Les milliers d'employés de l'agence, bien qu'ils puissent exercer une certaine autonomie dans la mise en relation d'informations ou la poursuite de certaines cibles, ne font qu'appliquer de manière technique et en des contextes spécifiques des directives générales décidées en amont dans un cadre stratégique. Il est possible de mettre en relation la structure décisionnelle et le mode de financement exogènes, c'est-à-dire que la source externe des ressources financières de l'agence – soit le budget voté au Congrès et une partie considérable du « budget noir[3] » – coïncide avec l'origine externe de la structure décisionnelle de l'organisation.

De la même façon, ce sont des investissements de provenance extérieure qui ont permis de financer le développement de l'algorithme *PageRank* du moteur de recherche Google, avant que l'entreprise n'opte pour un modèle d'affaires centré sur la publicité contextuelle. L'autonomie financière de l'entreprise ne fut possible qu'à partir du moment où Google développa une popularité suffisante pour générer une valeur endogène et une certaine indépendance

[3] Andrews, Wilson et Todd Lindeman, « The Black Budget ».

organisationnelle. Si l'état actuel du financement de Google constitue aujourd'hui une distinction importante par rapport à la NSA en matière d'autonomie, il demeure que la structure décisionnelle hétérodoxe de l'entreprise est analogue à celle de l'agence en raison de la concentration du pouvoir décisionnel entre les mains des gestionnaires. En effet, en dépit de l'entrée de Google sur le marché boursier en 2004, l'entreprise évite volontairement de soumettre ses orientations aux attentes des actionnaires et d'ainsi réduire son autonomie décisionnelle par la mise en place d'une structure d'actionnariat particulière :

> La structure standard de propriété publique peut compromettre l'indépendance et l'objectivité, qui ont été importantes aux réussites antérieures de Google et que nous considérons comme fondamentales à son avenir. Par conséquent, nous avons implémenté une structure corporative conçue pour protéger la capacité de Google à innover et à retenir ses caractéristiques les plus distinctives. […] À notre avis, les pressions externes cherchent trop souvent à dissuader les compagnies de poursuivre des opportunités à long terme pour correspondre aux prévisions trimestrielles du marché[4].

En somme, si l'autonomie financière des deux organisations est un facteur important de différenciation, celles-ci ont en commun une structure décisionnelle basée sur la définition des stratégies et des orientations par une minorité de gestionnaires et de responsables. La majeure partie des employés et des ressources humaines des deux organisations n'ont aucun pouvoir individuel ou collectif sur la direction et les fins qu'elles poursuivent. Il est aussi possible de souligner l'importance que revêt dans les deux cas l'automatisation logicielle des systèmes informatiques. Donc, en dépit des différences en matière d'imputabilité dérivées des axiomes capitalistes et sécuritaires, la structure décisionnelle élitiste et le recours important à l'automatisation technologique sont deux dimensions communes à Google et à la NSA.

4.4. Tactiques: différences et similitudes

Comme l'ont démontré les deux études de cas, les tactiques employées dans la surveillance des données personnelles sont diversifiées et propres à chacune des deux organisations. Néanmoins, il est possible de remarquer certains ressorts communs.

[4] Alphabet, « 2004 Founders' IPO Letter – ''An Owner's Manual'' for Google's Shareholders », *Alphabet Investor Relations*, s/d, URL : https://abc.xyz/investor/founders-letters/2004/ipo-letter.html (consulté le 10 août 2017).

4.4.1. Différences: rôle de l'individu et autonomie organisationnelle

D'abord, les tactiques de Google et de la NSA diffèrent dans le rôle qu'y joue l'individu. En ce qui concerne la fonction dévolue à l'individu dans le cas de Google, l'opération de la surveillance est intégrée aux interfaces de ses services. Par conséquent, les individus jouent un rôle crucial en autorisant de façon tacite leur propre surveillance en usant des logiciels de Google ; afin de s'y soustraire en grande partie, ceux-ci ont toujours la possibilité de cesser de les utiliser ou bien d'opter pour des alternatives. Dans le cas de la NSA, toutefois, la surveillance des données personnelles n'est pas dépendante du choix des individus en matière logicielle. Grâce à ses nombreux moyens, dont l'interception des flux de données en transit dans les câbles sous-marins, l'accès légal et limité aux registres et bases de données des entreprises, l'accès illégal et illimité aux systèmes internes de certaines entreprises et l'installation clandestine de logiciels-espions, la NSA est en mesure de priver l'individu moyen d'un quelconque pouvoir de se soustraire à la surveillance dans le cyberespace. Les tactiques utilisées se différencient donc par le rôle et la marge de manœuvre qu'elles laissent à l'individu dans la surveillance de ses données personnelles.

Ensuite, il existe également une différence importante au niveau de l'indépendance organisationnelle dans le déploiement des tactiques de surveillance des données. Dans le cas de Google, presque toutes les données collectées le sont par l'entreprise elle-même, au moyen de ses propres services, vers ses propres bases de données afin d'accroître la valeur de ses propres produits[5]. À l'inverse, la NSA dépend d'une multitude d'entreprises, non seulement en ce qui concerne ses partenariats et sa coopération légale, mais aussi au niveau de la sous-traitance et des contractants privés ayant un accès général ou partiel aux systèmes de l'agence. En effet, la NSA n'emploie directement qu'environ 30 000 personnes, alors qu'elle contracte une pluralité d'entreprises qui mettent à sa disposition environ 60 000 exécutants, techniciens et analystes issus, entre autres, de Booz Allen Hamilton, Northrop Grumman et SAIC[6].

[5] Il importe de préciser que Google procède par des investissements stratégiques auprès de start-ups prometteuses dont les technologies finissent souvent par être incorporées aux logiciels de l'entreprise – par exemple, ce fut le cas de *Keyhole*, qui servit à développer son service *Google Earth*.

[6] Il s'agit de trois entreprises majeures du secteur de la Défense étasunienne. Les chiffres sont tirés de : Harcourt, Bernard, *Exposed : Desire and Disobedience in the Digital Age*, 70.

4.4.2. Similitudes : profilage individuel automatisé et métadonnées

Deux aspects techniques rapprochent les tactiques autrement distinctes de Google de la NSA : l'utilisation heuristique des métadonnées ainsi que l'assemblage de « sosies de données » afin de prédire le risque individuel.

D'abord, la grande majorité de la surveillance des données pratiquée par Google et la NSA ne procède pas à partir du contenu des communications. En effet, la complexité de l'interprétation sémantique des communications proscrit son utilisation dans des contextes de surveillance de masse. Lorsqu'il est néanmoins nécessaire de procéder à une analyse de contenu, Google et la NSA ont recours à des logiciels de repérage automatisé de mots-clés définis au préalable, qui en cas de détection génèrent une alerte nécessitant une évaluation par un analyste. Par exemple, les courriels transitant par Gmail sont analysés par des systèmes automatisés qui peuvent repérer des mots associés à des lieux, des marchandises ou des activités criminelles. Toutefois, parmi les activités routinières des deux organisations, l'analyse de contenu est significativement moins importante que la mise en relation des métadonnées.

En effet, les métadonnées permettent de réaliser une « économie de la surveillance », puisqu'elles constituent des abstractions qui consolident les informations essentielles (par exemple, date, heure, adresse de protocole Internet, etc.) d'une communication en laissant de côté la matière incongrue de leur contenu. Non seulement les métadonnées ne bénéficient pas des protections constitutionnelles concernant le droit à la vie privée, mais elles facilitent grandement la mise en relation des données et la production d'inférence utile. En somme, les métadonnées sont parfaitement adaptées aux organisations bureaucratiques, puisqu'elles sont déjà standardisées et organisées en catégories :

> Une façon d'y penser est que les données sont le contenu, tandis que les métadonnées sont le contexte. Les métadonnées peuvent être beaucoup plus révélatrices que les données, particulièrement dans l'agrégat. […] Quand il y a des populations entières sous surveillance, les métadonnées sont bien plus significatives, importantes et utiles. Comme l'a dit l'ancien avocat général de la NSA Stewart Baker, ''les métadonnées vous disent absolument tout sur la vie de quelqu'un. Si vous avez assez de métadonnées, vous n'avez pas vraiment besoin du contenu''. En 2014, l'ancien directeur de la NSA et de la CIA Michael Hayden a remarqué : ''Nous tuons des gens sur la base des métadonnées''[7].

[7] Schneier, Bruce, *Data & Goliath – The Hidden Battles to Collect Your Data and Control Your World*, 23.

Les métadonnées sont idéales pour les processus de surveillance de masse, où le traitement approfondi du contenu des toutes les communications est – pour l'instant – impossible et contre-productif. En ce sens, les métadonnées peuvent être considérées comme des heuristiques communicationnelles, qui en tant que données résumant des données, rationalisent les processus de surveillance des organisations informationnelles.

Ensuite, les deux organisations ont recours au profilage individuel, bien qu'elles évaluent des risques différents : d'un côté, la propension à consommer certaines catégories de produits, et de l'autre, la propension à être impliqué dans des crimes ou des actes terroristes. Dans les deux cas, l'utilisation d'algorithmes permet de repérer des régularités et des anomalies dans les données collectées, ce qui fonde la faisabilité technique de la surveillance de masse profonde. En somme, la mise en relation de données dispersées permet de constituer des « sosies de données » dynamiques d'une grande utilité dans des contextes publicitaires, sécuritaires, électoraux, administratifs, etc. Les sosies de données ainsi constitués regroupent un ensemble de catégories aux modalités fluides, qu'il s'agisse de segmentations de marché et de types de consommateurs ou bien d'affiliation idéologique et d'association à certaines personnes et organisations d'intérêt. Dans cette situation, l'individu physique est d'une importance secondaire : ce qui compte dans la surveillance informatique, ce sont les traces numériques laissées derrière toute activité. Celles-ci alimentent les processus d'assemblage, de croisement et d'extrapolation des données qui permettent aux organisations de tirer des inférences qui soient utiles à leurs opérations, à défaut d'être scientifiques ou exactes.

Donc, en dépit des différences tactiques importantes entre les services de Google et les programmes de la NSA, notamment en ce qui concerne le rôle de l'individu et l'indépendance de l'organisation, toutes les deux ont en commun d'exploiter le potentiel heuristique des métadonnées, notamment dans la constitution de profils types et dans le repérage de régularités ou d'anomalies.

4.5. Stratégies centrées sur l'asymétrie et les réseaux

Les études de cas ont souligné deux axes importants des stratégies organisationnelles de Google et de la NSA: l'entretien de l'asymétrie informationnelle et le développement continuel d'un métapositionnement au sein des réseaux d'information.

D'abord, l'asymétrie informationnelle repose sur un principe simple qui oriente les stratégies des organisations, en particulier celles spécialisées dans l'information : d'une part, maximiser la transparence de l'environnement opérationnel en vue d'une prise de décision la plus informée possible, et d'autre part, conserver autant que possible l'opacité des processus internes de l'organisation afin de préserver sa compétitivité et sa marge de manœuvre. En somme, il s'agit d'organiser les circuits d'information de sorte que, d'une part, il puisse y entrer un maximum d'informations pertinentes aux opérations, et d'autre part, que ne puisse en sortir qu'un minimum d'informations filtrées en fonction des intérêts de l'organisation :

> C'est l'histoire platonicienne de l'anneau de Gygès : celui qui est invisible, et qui donc peut voir tout ce que font les autres à leur insu, dispose d'un avantage stratégique énorme. C'est le ressort central d'entreprises comme Google [...]. Elles disent qu'elles doivent leur richesse et leur succès au fait d'avoir les meilleurs analystes de données et les meilleurs algorithmes. Mais ce succès tient moins à des compétences spéciales qu'à une position de pouvoir particulière, qui leur permet de surveiller tout le monde en se soustrayant elles-mêmes aux regards[8].

L'asymétrie en matière de visibilité et d'information apparaît donc être un ressort central à la mise en œuvre de toute stratégie organisationnelle. Ce qui caractérise les cas de Google et de la NSA, c'est leur concentration inégalée du capital informationnel global au sein de structures dont le fonctionnement interne est voilé. En ce sens, les deux organisations se ressemblent à un niveau fondamental en ce qu'elles constituent des boîtes noires spécialisées dans la surveillance globale et massive des données personnelles. Par conséquent, elles jouissent d'un potentiel stratégique hautement élevé, puisqu'elles peuvent compter sur une connaissance avancée et multidimensionnelle de l'environnement informationnel, tout en s'assurant que leurs adversaires, compétiteurs et cibles n'accèdent pas à des informations qui leur permettent d'anticiper, de contrecarrer ou d'imiter leurs ambitions. En somme, la « position de pouvoir particulière » qu'occupent respectivement Google et la NSA repose sur la maximisation simultanée de la transparence environnementale et de l'opacité organisationnelle.

Le résultat de cette situation constitue ce que nous nommons le métapositionnement. Au sein d'un système informationnel global et universel comme Internet, composé d'une myriade de réseaux interconnectés, le pouvoir d'une organisation informationnelle est lié à sa capacité à intégrer

[8] Richard, Claire, « Surveiller, tout en se cachant, est la forme la plus haute du pouvoir », *L'Obs*, 26 août 2016, URL : http://tempsreel.nouvelobs.com/rue89/rue89-le-grand-entretien/20160826.RUE7798/surveiller-tout-en-se-cachant-est-la-forme-la-plus-haute-du-pouvoir.html#link_time=1472220110 (consulté le 28 octobre 2017).

d'autres réseaux au sein de ses propres circuits informationnels. En effet, en rassemblant l'information d'une multitude de réseaux externes (par exemple, sites web, bases de données, communications), l'organisation informationnelle peut s'approprier une partie de leur valeur sans assumer une part du risque inhérent à leur production[9]. Ainsi, Google entretient un métapositionnement par rapport à toutes les pages de la Toile publique, puisque son moteur de recherche constitue un portail assurant le relais entre les usagers et les informations produites et affichées sur les sites web. Ce faisant, Google engrange des revenus colossaux et génère une valeur commerciale inégalée sans avoir à produire la moindre information : le risque et le coût de la production d'information ne sont pas assumés par Google, tandis que l'entreprise s'arroge une partie notable de la valeur de la production intellectuelle sur la Toile – telle qu'elle se définit par la pertinence de l'information trouvée, par les revenus publicitaires et par l'attention des usagers.

D'une manière similaire, la NSA entretient un métapositionnement vis-à-vis des systèmes de communication électronique en général, en vertu non seulement de ses installations techniques destinées à l'interception, mais aussi de l'autorité légale qu'elle dérive de ses mandats exécutifs. Pour sa part, la NSA assure le relais entre les besoins informationnels stratégiques des institutions gouvernementales étasuniennes et la sphère globale des communications informatiques et satellites. La prédominance en matière d'interception et de surveillance de la sphère globale de l'information signifie que la NSA opère au niveau d'abstraction le plus élevé, ce qui contribue à l'ascendance stratégique du système gouvernemental étasunien sur le reste du monde, du moins en matière informationnelle. Grâce à un ensemble de partenariats, d'infrastructures, de logiciels spécialisés et de ressources financières, la NSA opère en amont de la plupart des autres institutions, dont les organisations internationales, les organisations non gouvernementales, les entreprises et les États non membres des « cinq yeux », puisqu'ils dépendent tous de la production, de la circulation et de la consommation d'information par des moyens informatiques ou satellitaires.

Toutefois, si la logique de métapositionnement au sein des réseaux informationnels est commune à Google et à la NSA, il demeure que leurs positions respectives ne sont pas égales ou équivoques. En effet, il est clair à partir des études de cas que la NSA opère en amont de Google, puisque l'entreprise fait elle-même partie des réseaux qui alimentent la métaposition occupée par

[9] Lanier, Jaron, *Who Owns the Future ?*, 61-62.

l'agence de renseignement. Nous constatons donc l'insertion de la métaposition de Google, établie par rapport à la majorité des autres services, sites web et données de la Toile publique, parmi les réseaux constitutifs de la métaposition de la NSA, établie par rapport aux autres organisations et structures informationnelles en tous genres[10].

5. Réflexions sur les résultats

En conclusion, les résultats des études de cas et de l'interprétation analytique soulignent la complexité des similitudes et des différences entre deux organisations informationnelles majeures aux États-Unis et dans le cyberespace, soit Google et la NSA. En particulier, les similitudes structurelles et contextuelles entre les deux organisations appuient un concept important recensé dans la revue de la littérature, soit celui d'une « nébuleuse de surveillance étatique et corporative ». De plus, l'importance des facteurs systémiques communs aux deux organisations, en dépit des cultures organisationnelles distinctes, justifie de considérer la littérature sur le conditionnement technologique afin de comprendre l'essor des pratiques de surveillance de masse des données personnelles.

5.1. Retour sur le concept de « nébuleuse de surveillance étatique et corporative »

D'abord, les études de cas appuient certains postulats du concept de « nébuleuse de surveillance étatique et corporative », notamment en ce qui concerne la convergence des intérêts, des méthodes et des structures opérationnelles entre les organisations informationnelles gouvernementales et privées. Les résultats tempèrent le cadrage de l'Internet en tant que structure fondamentalement émancipatrice pour les individus et déstabilisatrice pour les structures de pouvoir. En fait, les descriptions relatives à l'intégration et l'exploitation d'Internet en tant que vecteur d'extraction de données personnelles s'inscrivent dans l'idée que « le cyberespace n'était donc pas un espace révolutionnaire pour la subversion des structures de pouvoir existantes […], mais plutôt un champ pour la superposition des structures de pouvoir traditionnelles sur cette nouvelle surface[11] ». Il est possible d'affirmer que les structures ouvertes, universelles et circulatoires d'Internet permettent et facilitent l'essor et la normalisation des processus de surveillance de masse à une échelle comparable à celle des régimes totalitaires du 20e siècle. La

[10] À l'exception, entre autres, de certains États et agences de renseignement étrangères.
[11] Mc Evoy Manjikian, Mary, « From Global Village to Virtual Battlespace : The Colonizing of the Internet and the Extension of Realpolitik », 385.

mise en données par les technologies numériques et la circulation de ses données par les technologies réticulaires constituent deux avancées critiques qui transforment qualitativement et quantitativement les processus de surveillance caractéristiques de l'État moderne.

Néanmoins, les résultats ne permettent pas d'écarter l'idée que l'Internet soit aussi propice à une pluralité de formes de subversion institutionnelle et de résistance politique. Il est indéniable que la connexion théoriquement illimitée des individus entre eux à travers le monde peut être une condition catalytique favorable à des changements politiques, économiques, culturels et sociaux défavorables à la reproduction du contrôle social et du statu quo politico-économique. Toutefois, étant donné l'origine militaro-scientifique des technologies en question, il semble également indéniable que les stratèges des institutions militaires et des grandes organisations capitalistiques ont constaté eux-mêmes ce potentiel déstabilisateur et ont cherché à le minimiser dans la limite du possible – notamment par le recours à la surveillance de masse des données personnelles. En accroissant la pression et les risques de turbulence sur les structures traditionnelles de l'État et du capital, il est probable que l'effervescence sociopolitique populaire stimulée par Internet ait donné lieu au déploiement de nouvelles stratégies sécuritaires et commerciales destinées à circonscrire les directions possibles du développement du médium et à y reproduire l'ordre politico-économique existant.

La dualité du médium entre les possibilités de subversion et de reproduction de l'ordre politico-économique fait écho à la notion de technologie à double usage, soit l'usage militaro-politique et l'usage civil-commercial. En ce sens, il est possible d'illuminer le potentiel révolutionnaire et réactionnaire d'Internet par une analogie historique avec le réseau de routes bâti par l'Empire romain pour connecter ses régions à sa capitale[12]. Il existe des similitudes quant à l'usage double du réseau – physique – de routes et le réseau – virtuel – d'information. Dans les deux cas, le réseau a pour fonction manifeste de stimuler et d'accélérer la circulation des personnes, des biens, de l'information et du commerce : sa construction prend dès lors les apparences d'un bien public apolitique accroissant la prospérité générale en permettant aux périphéries d'être connectées au centre politique, économique, intellectuel et militaire. Toutefois, la fonction latente des deux réseaux est de rationaliser l'exercice du pouvoir par le centre, puisque les routes facilitent le déplacement des armées, des espions et des responsables romains ainsi que la gestion des flux

[12] Hardt, Michael et Antonio Negro, *Empire*, Harvard University Press, 2001, 298.

humains et matériels qui y circulent. Le réseau – physique et virtuel – est simultanément un facteur d'effervescence socioculturelle et de solidification de l'ordre politico-militaire dominant. Autrement dit, les routes – dallées et informationnelles – qui connectent les territoires sont à la fois des vecteurs de prospérité et de vulnérabilité, de mobilité et de contrôle : en ce sens, elles représentent des technologies à usage militaire et civil. Dans le cas du réseau informationnel, la NSA représente son versant militaire et Google son versant civil et commercial.

Au niveau subversif, Internet permet d'organiser un champ de liberté expressive, de mobilité informationnelle et d'interconnexion communicationnelle sans précédent, ayant pour effet d'accélérer et de rationaliser les processus socio-économiques des territoires ; au niveau reproductif, le réseau est une opportunité d'étendre, d'intensifier et d'automatiser les processus de surveillance des États industriels avancés et des grandes entreprises. Certes, le réseau n'est pas simplement soumis à la volonté des organisations étasuniennes ou occidentales : une fois constitué, l'espace informationnel étend la prospérité et la vulnérabilité à tous ceux qui y sont connectés – tout en marginalisant ceux qui ne le sont pas[13].

> Il n'y a pas ici un pouvoir qui est complètement entre les mains d'une personne qui puisse l'exercer seule et complètement sur les autres. C'est une machine dans laquelle tout le monde est pris, ceux qui exercent le pouvoir tout autant que ceux sur lesquels il s'exerce. […] Le pouvoir n'est plus substantiellement identifié avec un individu qui le possède ou l'exerce […] ; il devient une machinerie que personne ne détient. Certainement, tout le monde n'occupe pas la même position ; certaines positions sont prépondérantes et permettent de produire un effet de suprématie[14].

De manière paradoxale, Internet constitue une « machinerie » joignant dans ses structures la liberté subversive et la sécurité du système : elle stimule et encourage les libertés individuelles d'expression, d'association et d'accès à l'information, mais ceci à l'intérieur d'un cadre technique structuré en amont par la surveillance, la quantification et l'exploitation des données. Ces principes confèrent une « position prépondérante » aux grandes organisations ayant un capital technologique suffisamment important pour produire un « effet de suprématie ». Autrement dit, Internet décuple la portée et la complexité des activités communicationnelles des populations en aval de structures technocratiques organisées pour sécuriser, intégrer et analyser ces activités productrices de données personnelles: « la sécurité et la liberté sont conçues non pas comme des

[13] Hardt, Michael et Antonio Negro, *Empire*, 300.
[14] Foucault, Michel, *Power/Knowledge : Selected Interviews and Other Writings, 1972-1977*, 156.

principes opposés, mais comme des parties constitutives de la gouvernementalité libérale ; elles sont toutes deux des éléments d'une seule technologie de gouvernement[15] ».

En somme, l'Internet est un espace de gouvernementalité étendant le rapport entre sécurité et liberté à la sphère des communications. D'après le principe de la gouvernementalité libérale, l'intégration de la surveillance des données personnelles aux stratégies commerciales et sécuritaires permet d'« arranger les choses de façon à ce que la population, en ne suivant que son intérêt propre, agisse comme elle le doit[16] » par rapport aux intérêts organisationnels dominants. En effet, la dynamique des intérêts individuels conduit à une production continuelle et croissante de données personnelles, qui alimentent les processus d'acquisition d'information des grandes organisations. Autrement dit, en suivant son intérêt à communiquer et à accéder à l'information, la population contribue involontairement aux intérêts commerciaux et sécuritaires de Google et de la NSA. Donc, l'environnement artificiel et technique d'Internet et des services de Google est structuré de sorte à joindre la liberté individuelle à la sécurité organisationnelle par la surveillance des données personnelles.

Ces réflexions sur la dualité intrinsèque du médium éclairent la complémentarité de la surveillance commerciale et de la surveillance sécuritaire. La comparaison analytique des deux organisations soutient l'idée qu'elles jouent des rôles certes distincts, mais complémentaires du point de vue de la sécurisation d'Internet. Toutes deux étendent la portée politique de structures établies – l'État et l'entreprise – à un médium perturbateur et cherchent à y instaurer un ordre adapté à leurs intérêts organisationnels. D'un côté, l'image publique positive de Google, ainsi que les bénéfices tangibles offerts à ses usagers, incitent et stimulent la production et la circulation des données personnelles dans un cadre à priori apolitique, utilitaire et mutuellement avantageux : « Ces institutions [dont Google] incitent et amènent les usagers à exprimer leurs pensées et leurs idées à travers des appels à la participation, analysent ces expressions à la recherche de schémas de pensée, puis utilisent ces mêmes canaux pour amplifier les idées qu'elles désirent et ignorer les autres[17] ». Le versant civil et commercial du médium stimule la production populaire de données personnelles, qui sont ensuite captées et analysées par la surveillance commerciale et sécuritaire. En d'autres mots, dans l'économie politique des données personnelles, les activités de

[15] Lemke, Thomas, *Foucault, Governmentality, and Critique*, Routledge, 2015, 49.
[16] Scott, David, « Colonial Governmentality », 202.
[17] Gehl, Robert, « What's on your mind ? Social media monopolies and noopower ».

Google cadrent avec les intérêts de la NSA, qui n'est pas dans une position susceptible d'inciter – ou d'induire – les individus à procéder à la mise en données de leurs pensées, de leurs activités, de leurs relations sociales, de leurs préférences et de leurs habitudes : « en raison de l'économie politique des médias sociaux monopolistiques, Facebook, Google et Twitter se tournent de plus en plus vers leurs bienfaiteurs (gouvernements, entités globales comme l'Organisation internationale de la propriété intellectuelle, grands investisseurs et publicitaires) en matière de direction pour définir leurs accords de conditions d'utilisation et structurer leurs sites[18] ».

5.2. Conclusion : de l'autonomie et du conditionnement technologique

La conclusion sur la validité empirique du concept de « nébuleuse étatique corporative », soulignée par la complémentarité systémique entre Google et la NSA, permet de contribuer partiellement à l'enjeu plus large des déterminants technologiques sur la surveillance. En effet, les pratiques de surveillance de Google et de la NSA partagent de nombreuses similarités structurelles. En dépit des différences découlant des impératifs commerciaux et sécuritaires, elles ont en commun un objectif pouvant être qualifié de systémique : la collecte et l'analyse des données personnelles du plus grand nombre d'individus possible. Or, il apparaît peu vraisemblable que cet objectif commun soit tributaire d'une décision arbitraire prise par des responsables peu scrupuleux. Il est plus indiqué de considérer la présence d'un impératif structurel qui pèse sur les organisations informationnelles et auquel les responsables « doivent choisir » de se conformer afin de prospérer dans un contexte compétitif :

> Les individus et les élites sont présents, mais leurs rôles et actions se conforment de si près au cadre établi par les structures et les processus du système technique que toute prétention de détermination par décision humaine devient purement illusoire. […] Leur quête de pouvoir vient presque exclusivement d'une reconnaissance de ce qui est nécessaire à une performance efficiente dans un monde de technologie avancée. […] Si la technostructure de la compagnie X n'agit pas de façon créative au sein du contexte fixé par les impératifs technologiques, alors un groupe de prise de décision analogue dans la compagnie Y ou Z le fera certainement. La conduite d'une quelconque instance particulière d''intelligence organisée'' est simplement celle que toute intelligence du même type, préparée de façon similaire, suivrait dans les mêmes circonstances[19].

Les similitudes profondes remarquées entre des organisations à priori foncièrement différentes nous amènent à considérer que l'injonction à collecter et analyser le plus de données pertinentes

[18] Gehl, Robert, « What's on your mind ? Social media monopolies and noopower ».
[19] Winner, Langdon, *Autonomous Technology : Technics-out-of-Control as a Theme in Political Thought*, The MIT Press, 1978, 174.

possible découle du fait que les conditions technologiques le permettent. Dans cet ordre d'idée, il est pertinent de conclure la recherche par une brève réflexion sur le rôle du conditionnement technologique[20] dans l'essor de la surveillance informatique. Le facteur technologique permet de situer l'essor récent de la surveillance de masse des données personnelles dans un contexte plus large de compétition politique et économique, où Google et la NSA s'érigent comme les organisations informationnelles les plus créatives et les mieux adaptées aux conditions sociotechniques du 21e siècle.

Dans cette perspective, la surveillance de masse des données personnelles est une pratique organisationnelle rationnellement adaptée aux possibilités offertes par les technologies informatiques et réticulaires. En effet, les gains en efficience économique et sécuritaire que cette pratique génère s'inscrivent en continuité avec l'histoire du progrès technique. En considérant le prolongement indéfini des dynamiques de rationalisation technique amorcées par la révolution industrielle, le philosophe critique Jacques Ellul anticipait de plus de quatre décennies l'avènement d'une surveillance de masse aux visées non pas répressives, mais fonctionnelles :

> Plus nous mobilisons les forces de la nature, plus nous devons mobiliser les individus et plus nous requérons l'ordre, qui aujourd'hui représente la valeur la plus élevée. […] Pour être certain d'appréhender les criminels, il est nécessaire que *tout le monde* soit supervisé. Il est nécessaire de savoir exactement ce que fait chaque citoyen, de connaître ses relations, ses loisirs, etc. Et l'État est de plus en plus dans une position de connaître ces choses. Ceci n'implique pas un règne de terreur ou d'arrestations arbitraires. La meilleure technique est celle qui se fait le moins sentir et qui représente le moins grand fardeau. Mais chaque citoyen doit être profondément connu […] et doit vivre sous des conditions de surveillance discrète. Tout cela résulte de la perfection des méthodes techniques[21].

La perspective structurelle ne se résume pas à considérer la technologie comme une force monolithique, indépendante et autonome qui puisse elle-même expliquer la surveillance de masse. Il s'agit plutôt de percevoir que les conditions existantes du développement technologique constituent un horizon d'action stratégique, au sein duquel évoluent des organisations prêtent à adapter leurs pratiques à ses possibilités afin de maximiser leur potentiel et leur pouvoir. En ce sens, l'état du développement technologique agit comme une variable susceptible d'infléchir la

[20] Cette notion est préférable au terme « déterminisme technologique », puisque celui-ci peut laisser l'impression que le développement technologique est causalement antécédent au monde social.
[21] Ellul, Jacques. *The Technological Society*, 100-103.

forme et la structure des activités humaines – incluant les pratiques de collecte d'information et surveillance :

> Les idées, datées et traditionnelles, de pensées et d'actions privées et isolées – les schémas des technologies mécaniques – sont très sérieusement menacées par les nouvelles méthodes de récupération électrique et instantanée d'information, par la banque de données électriquement informatisée – cette grande colonne à commérages qui ne pardonne pas, n'oublie pas et de laquelle il n'y a pas de salut, pas d'effacement des 'erreurs' précoces[22].
>
> Dans le monde de l'encre et du papier, les documents sont groupés en dossier, les dossiers sont mis en boîte, les boîtes sont entreposées ou jetées. Les capacités de recherche et de traitement des informations sont, par conséquent, limitées par le coût et l'importante difficulté d'entreposer, de trouver, de chercher et de traiter un grand nombre de dossiers sur papier. Cet inconvénient fonctionne en tant que mécanisme par lequel le système oublie l'information passée, de manière analogue à la façon dont nous oublions nous-mêmes. Toutefois, l'histoire est très différente dans le monde numérique ; l'information numérisée est facile à entreposer, facile à chercher et à traiter, ainsi que peu coûteuse à conserver sur des périodes de temps étendues. Les systèmes d'information numériques tendent, par conséquent, à collecter une grande quantité d'information accessoire et à retenir cette information indéfiniment[23].

L'apport des considérations sur le conditionnement technologique est de permettre de comprendre les activités de surveillance de masse de Google et de la NSA en tant que stratégies adaptées à l'exploitation maximale des nouvelles conditions sociotechniques. En particulier, les dynamiques de compétition capitaliste et interétatique tendent vers l'exploitation maximale du potentiel technologique. De ce point de vue, il apparaît mal indiqué de juger des activités de Google et de la NSA sur un plan moral et civique, alors que toutes deux sont des organisations technologiques structurées et définies avant tout par le critère d'efficience. En effet, il apparaît clair que si Google décidait de réduire sa collecte ou de permettre aux individus de s'y soustraire, non seulement l'entreprise perdrait-elle une grande partie de son chiffre d'affaires, mais elle serait inévitablement dépassée par une autre entreprise prête à exploiter pleinement le potentiel des données personnelles. De même, une réduction substantielle des programmes de collecte de la NSA réduirait vraisemblablement sa capacité à remplir les conditions de son mandat institutionnel. La réalité de la compétition interpersonnelle et organisationnelle fait en sorte que le principe d'efficience prend préséance sur les considérations morales ou civiques: « Le cœur du problème économique s'est déplacé à la pointe extrême du développement technique. Le vrai

[22] McLuhan, Marshall et Quentin Fiore, *The Medium is the Massage – An Inventory of Effects*, 12.

[23] Blanchette, Jean-François et Deborah Johnson, « Cryptography, data retention, and the panopticon society (abstract) », *Computers and Society*, vol. 28, n. 2, juin 1998, 1.

débat concerne qui sera dans une position d'appuyer, absorber et intégrer le progrès technique et de fournir les conditions optimales à son développement[24] ».

C'est d'ailleurs cette préséance du critère d'efficience qui explique pourquoi des masses d'usagers utilisent les services de Google tout en sachant qu'ils cèdent leurs données personnelles à l'entreprise. Dans cet ordre d'idées, l'individu rationnel recherche la simplicité et l'efficience dans ses activités, ce qui signifie que son autonomie tend vers des comportements normalisés qui cadrent avec les intérêts des organisations politiques et économiques, au premier chef les États et les entreprises. Ceci permet de comprendre sociologiquement le processus par lequel des centaines de millions d'individus libres et autonomes choisissent rationnellement de se soumettre à une surveillance profonde, indéfinie et multiple en contrepartie de l'efficience tangible offerte par l'utilisation d'Internet. Dans la même logique, les organisations spécialisées dans l'information choisissent rationnellement de développer des logiciels et des systèmes coûteux capables de collecter, de traiter et d'analyser des quantités colossales d'informations personnelles en vue d'accroître la valeur et le potentiel de leurs activités. Cette confluence d'intérêt structurée par l'efficience explique autant la soumission personnelle à la surveillance, parfois décrite en termes d'apathie et d'indifférence civique, que la constitution étatique et corporative de vastes systèmes de surveillance personnelle, parfois conçue comme une dérive autoritaire ou un abus de pouvoir. Or, il importe de préciser que les populations d'usagers et les organisations de surveillance suivent toutes deux leur propre intérêt tel que défini à la lumière des conditions technologiques existantes.

Donc, il semble que l'autonomie et le conditionnement technologique soient des notions plus interdépendantes qu'il ne paraît de prime abord, ce qui rejoint en partie le propos sur la jonction de la liberté et de la sécurité par la surveillance informatique. Dans les deux cas, l'ambiguïté constatée soutient l'idée que la liberté et l'autonomie ne sont pas strictement opposées à la sécurité et au conditionnement technologique, mais qu'elles sont plutôt un point crucial de leur exercice ; d'autant plus que les individus ne sont pas simplement des sujets des structures de pouvoir, mais jouent un rôle dans ses opérations[25]. Il semble y avoir une importance dynamique

[24] Ellul, Jacques. *The Technological Society*, 198.
[25] Rose, Nikolas et Peter Miller, « Political Power Beyond the State: Problematics of Government », *The British Journal of Sociology*, vol. 43, n. 2, 1992, 174.

d'interdépendance, où la sécurité et le conditionnement ne s'exercent pas contre, mais à travers la liberté et l'autonomie personnelle[26].

Manifestement, la piste du conditionnement technologique mérite d'être considérée par de prochaines recherches, nonobstant la littérature déjà considérable et les controverses qu'elle peut soulever face aux postulats des cultures libérales. À l'ère cybernétique, caractérisée par l'intégration des populations au sein d'un médium global qui défie les notions préétablies de temps, d'espace, de liberté, de sécurité, d'autonomie et de conditionnement, le besoin se fait sentir de mettre à jour notre compréhension du politique et de l'individu face à de vastes systèmes d'information instantanés, continus et ubiquitaires.

5.3. Considérations sur la validité interne et externe de la recherche

Les descriptions et analyses du présent mémoire visent à saisir et représenter le contexte et les pratiques de l'entreprise Google et de la NSA en ce qui concerne la surveillance des données personnelles des populations mondiales. Comme dans toute étude qualitative, il importe que les descriptions faites correspondent au réel par l'usage d'une méthode reproductible. Dans notre démarche, nous avons procédé à deux études de cas descriptives menant à un chapitre comparatif et analytique. Notre approche idiographique signifie que nous avons cherché à cerner les aspects uniques et caractéristiques des pratiques de surveillance en appliquant un même schéma descriptif : le contexte dans lequel s'inscrivent les pratiques, les types de données qu'elles ciblent, les principes qui les sous-tendent, les tactiques par lesquelles elles s'opèrent et les stratégies qu'elles servent. Ce schéma descriptif cherche à circonscrire le phénomène en l'abordant de différents angles capables d'illuminer des dimensions distinctes, mais connexes. Il existe certainement des alternatives méthodologiques pertinentes pour étudier ces pratiques ; notre choix répond d'une volonté de représenter les dimensions sociales, techniques et politiques des pratiques de surveillance. Ce faisant, nous avons renoncé à une description en profondeur qui se serait concentrée sur un seul aspect du phénomène.

En ce qui concerne la validité interne des résultats, la méthode utilisée permet de représenter le réel de façon valide, bien que partielle. D'autres dimensions du phénomène auraient pu être ajoutées, ce qui constitue une faiblesse intrinsèque à la tâche de circonscrire un terrain d'étude

[26] Rose, Nikolas et Peter Miller, « Political Power Beyond the State: Problematics of Government », 174.

dans le foisonnement des phénomènes sociaux. Toutefois, parmi les dimensions présentées et décrites, notre recours aux documents primaires des deux organisations permet de croire que nous accédons à la réalité des pratiques concernées ; notre recours complémentaire à la littérature scientifique et à la couverture journalistique des deux organisations a permis de trianguler le sujet en bonifiant notre traitement du sujet de perspectives extérieures et éclairées.

En ce qui concerne la validité externe des résultats, la situation est plus mitigée. D'une part, les deux organisations étudiées occupent des positions sociotechniques et politiques privilégiées qui n'ont pas d'équivalent exact. En ce sens, les résultats des études de cas et de la comparaison analytique ne peuvent pas être transposés de façon intacte à d'autres organisations ne jouissant pas de la même supériorité technologique. En tant qu'organisations informationnelles les plus développées dans leurs champs respectifs, Google et la NSA possèdent des caractéristiques uniques qui reflètent leur stade de développement. D'autre part, ces positions privilégiées constituent des idéaux types qui illustrent les dynamiques de surveillance des données dans leur plein déploiement ; d'autres entreprises et d'autres agences ont certainement des modèles d'affaires et des programmes analogues, mais de moindres ampleurs. En d'autres mots, sans s'appliquer tous azimuts aux autres organisations informationnelles, les résultats représentent vraisemblablement des tendances appelées à croître en fonction des possibilités technologiques et de l'intégration des populations au cyberespace. Si des organisations aux moyens et aux activités similaires à ceux de Google et de la NSA émergeaient, il est raisonnable de penser que les résultats analytiques demeureraient pertinents, bien qu'incomplets. Les pratiques sociotechniques étant contingentes et socialement situées – et la surveillance des données n'y faisant pas exception – il est certain que les résultats de la recherche ne pourraient pas représenter complètement la réalité des pratiques de ces autres organisations. Après tout, la démarche idiographique n'est pas propice à la généralisation des résultats, mais plutôt à l'exposition approfondie d'un cas en particulier. En contribuant à l'avancement des connaissances des pratiques de surveillance de Google et de la NSA, nous voulons éclairer le phénomène de la surveillance informatique de masse à travers ses deux organisations les plus sophistiquées. D'autres recherches sont à faire pour comprendre les processus de surveillance qui évoluent en deçà des apex ici étudiés.

Bibliographie

Agazzi, Evandro, « From Technique to Technology : The Role of Modern Science », *Philosophy & Technology*, vol. 2, n. 4, hiver 1998, URL : http://scholar.lib.vt.edu/ejournals/SPT/v4_n2pdf/AGAZZI.PDF (consulté le 4 décembre 2017).

Agger, Ben, *Postponing the Postmodern : Sociological Practices, Selves, and Theories*, Rowman & Littlefield, 2002.

Alphabet Investor Relations, *Press Release – Alphabet Announces Fourth Quarter and Fiscal Year 2015 Results*, 2016, URL https://abc.xyz/investor/news/earnings/2015/Q4_google_earnings/index.html (consulté le 11 mars 2017) ;

Alphabet, « 2004 Founders' IPO Letter – ''An Owner's Manual'' for Google's Shareholders », *Alphabet Investor Relations*, s/d, URL : https://abc.xyz/investor/founders-letters/2004/ipo-letter.html (consulté le 10 août 2017).

Ambinder, Marc, « Sources : NSA sucks in data from 50 companies », *The Week*, 6 juin 2013, URL : http://theweek.com/articles/463456/sources-nsa-sucks-data-from-50-companies (consulté le 24 juin 2017).

American Civil Liberties Union, *NSA Documents Released to the Public Since June 2013*, URL www.aclu.org/nsa-documents-released-public-june-2013 (consulté le 1 décembre 2017).

Amoore, Louise, « Biometric Borders : Governing mobilities in the war on terror », *Political Geography*, n. 25, 2006, 336-351.

Anderson, Sheldon, « Metternich, Bismarck, and the Myth of the ''Long Peace'', 1815-1914 », *Peace & Change*, vol. 32, n. 3, juillet 2007, 301-328.

Andrejevic, Mark, « Exploitation in the data-mine », chapitre dans C. Fuchs, K. Boersma, A. Albrechtslung et M. Sandoval, *Internet and Surveillance : The Challenges of Web 2.0. and Social Media*, Routledge, 2012, 71-88..

Andrejevic, Mark, « The Work of Watching One Another : Lateral Surveillance, Risk, and Governance », *Surveillance & Society*, vol. 2, n. 4, 2005, 479-497.

Andrews, Wilson et Todd Lindeman, « The Black Budget », *The Washington Post*, 29 août 2013, URL : http://www.washingtonpost.com/wp-srv/special/national/black-budget/ (consulté le 28 octobre 2017).

Angwin, Julia *et al.*, « AT&T Helped U.S. Spy on Internet on a Vast Scale », *The New York*

Times, 15 août 2015, URL : https://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html (consulté le 28 juin 2017).

Angwin, Julia, Charlie Savage *et al.*, « AT&T Helped U.S. Spy on Internet on a Vast Scale », *The Guardian*, 15 août 2015, URL http://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html?_r=0 (consulté le 1 décembre 2017).

Anthony Maurno, Dann et Louis Sirico, *Thin Air : How Wireless Technology Supports Lean Initiatives*, CRC Press, 2010.

Armbrust, Michael *et al.*, *Above the Clouds : A Berkeley View of Cloud Computing*, University of California at Berkeley, 10 février 2009, URL http://home.cse.ust.hk/~weiwa/teaching/Fall15-COMP6611B/reading_list/AboveTheClouds.pdf (consulté le 13 mars 2017).

Arora, Rahul, « Encyclopaedic Dictionary of Organization Behaviour », vol. 2, Sarup & Sons, 2000.

Arquilla, John, « The Strategic Implications of Information Dominance », *Strategic Review*, vol. 22, n. 3, 1994, 24-30.

Arthur, Charles, « NSA scandal : what data is being monitored and how does it work? », *The Guardian*, 7 juin 2013, URL : https://www.theguardian.com/world/2013/jun/07/nsa-prism-records-surveillance-questions (consulté le 14 juin 2017).

Austin, Lisa, « Lawful Illegality : What Snowden Has Taught Us about the Legal Infrastructure of the Surveillance State », chapitre dans Michael Geist et Wesley Wark, *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, Ottawa, University of Ottawa Press, 2015, 115-116.

Australian Law Reform Commission, « 9. Overview : Impact of Developing Technology on Privacy », *ALRC Report 108*, 2008, URL www.alrc.gov.au/publications/9.%20Overview%3A%20Impact%20of%20Developing%20Technology%20on%20Privacy/data-matching-and-data-mining (consulté le 1 décembre 2017).

Ball, James, « NSA stores metadata of millions of web users for up to a year, secret files show », *The Guardian*, 30 septembre 2013, URL : https://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents (consuté le 24 juin 2017).

Ball, Kirstie et David Murakami Wood, « Editorial : Political Economies of Surveillance », *Surveillance & Society*, n. 1-2, vol. 11.

Ball, Kirstie et Laureen Snider, *The Surveillance-Industrial Complex : A Political Economy of Surveillance*, Routledge, 2013.

Bamford, James, « The NSA is building the country's biggest spy center (watch what you say) », *Wired*, 15 mars 2012, URL : https://www.wired.com/2012/03/ff_nsadatacenter/ (consulté le 9 juin 2017).

Bauman, Zygmunt *et al.*, « After Snowden : Rethinking the Impact of Surveillance », *International Political Sociology*, n. 8, 2014, 121-144.

Bélanger, André-J, « Épistémologues de la science politique à vos marques! », chapitre dans Lawrence Olivier, Guy Bédard et Jean-François Thibault, *Épistémologie de la Science Politique*, Presses de l'Université du Québec, 1998.

Blanchette, Jean-François et Deborah Johnson, « Cryptography, data retention, and the panopticon society (abstract) », *Computers and Society*, vol. 28, n. 2, juin 1998, 1-2.

Bohman, James, « Critical Theory », dans *Stanford Encyclopedia of Philosophy* [en ligne], 2016, URL http://plato.stanford.edu/entries/critical-theory/ (consulté le 1 décembre 2017).

Boulanger, Philippe, *Géopolitique des médias : Acteurs, Rivalités et Conflits*, Armand Colin, 2014.

Built With, *Websites using Google AdSense*, 2017, URL https://trends.builtwith.com/websitelist/Google-Adsense (consulté le 9 mars 2017).

Bunker, Guy et Darren Thomson, *Delivering Utility Computing : Business-driven IT Optimization*, Wiley, 2006.

Carr, Nicholas, *The Big Switch : Rewiring the World, from Edison to Google*, W.W. Norton & Company, 2008.

Carroll, Rory, « Welcome to Utah, the NSA's desert home for eavesdropping on America », *The Guardian*, 14 juin 2013, URL : https://www.theguardian.com/world/2013/jun/14/nsa-utah-data-facility (consulté le 9 juin 2017).

Carroll, William et Colin Carson, « Neoliberalism, capitalist class formation and the global network of corporations and policy groups », chapitre dans Dieter Plehwe, Bernhard Walper et Gisela Neunhöffer, *Neoliberal Hegemony : A Global Critique*, Routledge, 2007.

Cerny, Philip, « Dilemmas of Operationalizing Hegemony », chapitre dans Mark Haugaard et Howard Lentner, *Hegemony and Power : Consensus and Coercion in Contemporary Politics*, Lexington Books, 2006.

Ciampaglia, Giovanni, Alessandro Flammini et Filippo Menczer, « The Production of Information in the Attention Economy », *Scientific Reports*, vol. 5, n. 9452, 2015, URL https://www.nature.com/articles/srep09452 (consulté le 2 juin 2017).

Clarke, Roger, « Information technology and dataveillance », *Communications of the ACM*, vol. 31, n. 5, 1988, 498-512.

Cohen, Tom, « Obama approves extension of expiring Patriot Act provisions », *CNN*, 27 mai 2011, URL : http://www.cnn.com/2011/POLITICS/05/27/congress.patriot.act/index.html (consulté le 29 juillet 2017).

Crampton, W. Jeremy, *The Political Mapping of Cyberspace*, University of Chicago Press, 2003.

Cruise O'Brien, Rita et G. K. Helleiner, « The Political Economy of Information in a Changing International Economic Order », *International Organization*, vol. 34, n. 4, 1980, 445-470.

Cueva, Mateo, « Cyber-Léviathan », *Société de l'information et coopération internationale*, vol. 22, n. 2, 2003, 233-250.

Curry, Edward, « The Big Data Value Chain : Definitions, Concepts, and Theoretical Approaches », chapitre dans José Maria Cavanillas, Edward Curry et Wolfgang Wahlster, *New Horizons for a Data-Driven Economy*, Springer Open, 2016.

Degli Esposti, Sara, « When Big Data meets dataveillance : the hidden side of analytics », *Surveillance and Society*, vol. 12, n. 2, 209-225.

Deibert, Ronald, « Black Code : Censorship, Surveillance, and the Militarisation of Cyberspace », *Millenium – Journal of International Studies*, vol. 32, n. 3, 501-530.

Deleuze, Gilles et Felix Guattari, *A Thousand Plateaus*, University of Minnesota Press, 1987.

Deleuze, Gilles, « Postscript on the societies of control », *October*, vol. 59, hiver 1992, 3-7.

Devereaux, Ryan, Glenn Greenwald et Laura Poitras, « Data pirates of the Caribbean », *The Intercept*, 19 mai 2014, URL : https://theintercept.com/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/ (consulté le 5 juillet 2017).

Dodge, Martin et Rob Kitchin, *Mapping Cyberspace*, Routledge, 2003.

Edelson, Chris, *Power Without Constraint : The Post-9/11 Presidency and National Security*, Wisconsin, University of Wisconsin Press, 2016.

Ellul, Jacques. *The Technological Society*, Vintage Books, 1964.

Elmer, Greg, *Profiling Machines : Mapping the Personal Information Economy*, The MIT Press, 2004.

Emmons, Alex, « Obama opens NSA's vast trove of warrantless data to entire intelligence community, just in time for Trump », *The Intercept*, 13 janvier 2017, URL : https://theintercept.com/2017/01/13/obama-opens-nsas-vast-trove-of-warrantless-data-to-entire-intelligence-community-just-in-time-for-trump/ (consulté le 28 juin 2017).

Encyclopaedia Britannica, « Moore's law », *Encyclopedia Britannica*, s/d, URL www.britannica.com/topic/Moores-law (consulté le 1 décembre 2017).

Engelhardt, Tom. *Shadow Government – Surveillance, Secret Wars, and a Global Security State in a Single-Superpower World*, Haymarket Books, 2014.

Fallows, James, « Facebook, Google, and the Future of the Online 'Commons' », *The Atlantic*, 3 février 2012, URL https://www.theatlantic.com/technology/archive/2012/02/facebook-google-and-the-future-of-the-online-commons/252522/ (consulté le 8 mars 2017).

Fallows, James, « The Dustbin of History : The Military-Industrial Complex », *Foreign Policy*, 2009, URL : http://foreignpolicy.com/2009/11/09/the-dustbin-of-history-the-military-industrial-complex/ (consulté le 8 juin 2017).

Farrell, Paul. « History of 5-Eyes – explainer », *The Guardian*, 2 décembre 2013, URL http://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer (consulté le 1 décembre 2017)

Fidler, David, *The Snowden Reader*, Indiana University Press, 2015.

Fisher, Louis, « State Secrets Privilege », *Library of Congress*, 2015, URL : https://www.loc.gov/law/help/usconlaw/state-privilege.php (consulté le 26 juin 2017).

Follorou, Jacques et Glenn Greenwald, « France in the NSA's crosshair : Wanadoo and Alcatel targeted », *Le Monde*, 21 octobre 2013, URL : http://www.lemonde.fr/technologies/article/2013/10/21/france-in-the-nsa-s-crosshair-wanadoo-and-alcatel-targeted_3499739_651865.html (consulté le 6 juillet 2017).

Ford, Gerald, « American Telephone and Telegraph Subpoena, 6/76 (2) », *The White House*, Washington, D.C., 1976, URL : https://www.fordlibrarymuseum.gov/library/document/0014/19077243.pdf (consulté le 2 juillet 2017).

Forgang, Jonathan, « ''The Right of the People'' : The NSA, the FISA Amendments Act of 2008, and Foreign Intelligence Surveillance of Americans Overseas », *Fordham Law Review*, vol.

78, n. 1, 2009, 217-266.

Foucault, Michel, *Power/Knowledge : Selected Interviews and Other Writings, 1972-1977*, Pantheon Books, 1980.

Foucault, Michel, *Security, Territory, Population*, Palgrave MacMillan, 2009.

Friedersdorf, Conor, « Why Does Anyone Trust the National-Security State ? », *The Atlantic*, 13 novembre 2013, URL : http://www.theatlantic.com/politics/archive/2013/11/why-does-anyone-trust-the-national-security-state/281429/ (consulté le 4 décembre 2017).

Fuchs, Christian, « The Political Economy of Privacy on Facebook », *Television New Media*, vol. 13, n. 2, 139-159.

Fuchs, Christian, *Social Media : A Critical Introduction*, SAGE, 2013.

Fuchs, Christian. *Internet and Society : Social Theory in the Information Age*, Routledge, 2008.

Gallagher, Ryan et Henrik Moltke, « Titanpointe – The NSA's Spy Hub in New York, Hidden in Plain Sight », *The Intercept*, 16 novembre 2016, URL : https://theintercept.com/2016/11/16/the-nsas-spy-hub-in-new-york-hidden-in-plain-sight/ (consulté le 2 juillet 2017).

Gallagher, Sean, « Building a panopticon : The evolution of the NSA's XKeyscore », *Ars Technica*, 9 août 2013, URL : http://arstechnica.com/information-technology/2013/08/building-a-panopticon-the-evolution-of-the-nsas-xkeyscore/

Ganasca, Jean-Gabriel, *Le mythe de la singularité*, Éditions du Seuil, 2017.

Gandy, H. Oscar, « The Political Economy of Personal Information », chapitre dans Janet Wasko, Graham Murdock et Helena Sousa, *The Handbook of Political Economy of Communications*, Blackwell Publishing, 2011.

Garrie, Daniel, « The Need for Private-Public Partnerships Against Cyber Threats – Why A Good Offense May Be Our Best Defense », *Huffinton Post*, 4 janvier 2016, URL www.huffingtonpost.com/daniel-garrie/the-soft-power-war-isis-d_b_8818866.html (consulté le 1 décembre 2017).

Gehl, Robert, « Knowledge Management Systems and Remote Control : Noopower and the Contemporary Transnational Corporation », dans Robert MacDougall, *Communication and Control*, Lexington Books, 2015.

Gehl, Robert, « What's on your mind ? Social media monopolies and noopower », *First Monday*, vol. 18, n. 3, 2013, URL http://firstmonday.org/article/view/4618/3421 (consulté le 13 février 2017).

Gellman, Barton et Ashkan Soltani, « NSA infiltrates links to Yahoo!, Google data centers worldwide, Snowden documents say », *The Washington Post*, 30 octobre 2013, URL : https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-Yahoo!-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html?utm_term=.b1e758ad97fc (consulté le 4 juillet 2017).

Gellman, Barton et Ashkan Soltani, « NSA surveillance program reaches 'into the past' to retrieve, replay phone calls », *The Washington Post*, 18 mars 2014, URL : https://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html?utm_term=.b3d6d2877fa1 (consulté le 5 juillet 2017).

Gellman, Barton et Ashkan Soltani, « NSA tracking cellphones locations worldwide, Snowden documents show », *The Guardian*, 4 décembre 2013, URL : https://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html?utm_term=.d251d6862da5 (consulté le 11 juin 2017).

Gellman, Barton et Laura Poitras, « U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program », *The Washington Post*, 6 juin 2013, URL : https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_print.html (consulté le 5 juillet 2017).

Gellman, Barton et Matt DeLong, « The NSA's three types of cable interception programs », *The Washington Post*, s/d, URL : http://apps.washingtonpost.com/g/page/world/the-nsas-three-types-of-cable-interception-programs/553/ (consulté le 3 juillet 2017).

Gellman, Barton et Todd Lindeman, « Inner workings of a top-secret spy program », *The Washington Post*, 29 juin 2013, URL : https://www.washingtonpost.com/apps/g/page/national/inner-workings-of-a-top-secret-spy-program/282/ (consulté le 3 juillet 2017).

Gibson, Owen, « The Story of the Long Tail », *The Guardian*, 10 juillet 2006, URL https://www.theguardian.com/media/2006/jul/10/mondaymediasection5 (consulté le 15 mars 2017).

Giddens, Anthony, *The Nation-State and Violence : Volume Two of a Contemporary Critique of Historical Materialism*, Polity Press, 1985.

Gillespie, Tarleton, « The Relevance of Algorithms », chapitre dans Tarleton Gillespie, Pablo Boczkowski et Kirsten Foot, *Media Technologies – Essays on Communication, Materiality, and Society*, MIT Press, 2014.

Gilliom, John, « Struggling with Surveillance : Resistance, Consciousness, and Identity », chapitre dans Richard Victor Ericson et Kevin Haggerty, *The New Politics of Surveillance and Visibility*, University of Toronto Press, 2006.

Gilpin, Robert, *US Power and the Multinational Corporation*, Basic Books, 1975.

Girard, Bernard, *The Google Way : How One Company is Revolutionizing Management as We Know It*, No Starch Press, 2009.

Goldsmith, A. J., « Policing new visibility », *British Journal of Criminology*, vol. 50, n. 5, 914-934.

Gonzales, Alberto, *Letter to Chairman Leahy and Senator Specter*, Washington D.C., The Attorney General, 17 janvier 2007, URL : http://graphics8.nytimes.com/packages/pdf/politics/20060117gonzales_Letter.pdf (consulté le 27 juin 2017).

Google, « How Search Works », *Google Inside Search*, 2016, URL http://www.google.com/insidesearch/howsearchworks/thestory/ (consulté le 4 décembre 2017).

Google, *AdSense Help – Managing websites – About the AdSense crawler*, 2017, URL https://support.google.com/adsense/answer/99376?hl=en (consulté le 9 mars 2017).

Google, *AdWords Help – Setup and Basics – Where your ads can appear*, 2017, URL https://support.google.com/adwords/answer/1704373?hl=en (consulté le 9 mars 2017).

Google, *Conditions d'utilisation de Google*, 2014, URL https://www.google.com/intl/fr/policies/terms/ (consulté le 6 mars 2017).

Google, *Economic Impact*, 2016, URL https://economicimpact.google.com/#/ (consulté le 1 décembre 2017).

Google, *Inside Search – How Search Works – The Story*, 2017, URL https://www.google.ca/insidesearch/howsearchworks/thestory/ (consulté le 4 mars 2017).

Google, *Our story – From the garage to the Googleplex*, 2017, URL https://www.google.com/about/our-story/ (consulté le 8 mars 2017).

Google, *Privacy & Terms – Partners – How Google uses data when you use our partners' sites or apps*, 2017, URL http://www.google.com/policies/privacy/partners/ (consulté le 10 mars 2017).

Google, *Règles de confidentialité et conditions d'utilisation – Comment nous utilisons les données que nous collectons*, 2017, https://www.google.com/intl/fr/policies/privacy/ (consulté le 11 mars 2017).

Google, *Technology Overview*, 4 juin 2011, URL https://web.archive.org/web/20110604120221/http://www.google.com/about/corporate/company/tech.html (consulté le 9 mars 2017).

Great Britain Competition Commission, *Classified Directory Advertising Services Provisional Findings*, The Stationery Office, 2006.

Greenwald, Glenn et James Ball, « The top secret rules that allow NSA to use US data without a warrant », *The Guardian*, 20 juin 2013, URL : https://www.theguardian.com/world/2013/jun/20/fisa-court-nsa-without-warrant (consulté le 22 juin 2017).

Greenwald, Glenn et Spencer Ackerman, « NSA collected US email records in bulk for more than two years under Obama », *The Guardian*, 27 juin 2013, URL : https://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama (consulté le 11 juin 2017).

Greenwald, Glenn, « Fisa court oversight : a look inside a secret and empty process », *The Guardian*, 19 juin 2013, URL : https://www.theguardian.com/commentisfree/2013/jun/19/fisa-court-oversight-process-secrecy (consulté le 27 juin 2017).

Greenwald, Glenn, « NSA collecting phone records of millions of Verizon customers daily », *The Guardian*, 6 juin 2013, URL : https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (consulté le 11 juin 2017).

Greenwald, Glenn, *No Place to Hide*, Random House, 2014.

Grunes, Allen, « Google's Quiet Dominance Over The 'Ad Tech' Industry », *Forbes*, 26 février 2015, URL www.forbes.com/sites/realspin/2015/02/26/googles-quiet-dominance-over-the-ad-tech-industry/#1e6d31215b78 (consulté le 4 mars 2017).

Guston, David, « The essential tension in science and democracy », *Social Epistemology : A Journal of Knowledge, Culture and Policy*, vol. 7, n. 1, 1993, 3-23.

Haggerty, Kevin et Richard Ericson, « The Surveillant Assemblage », *British Journal of Sociology*, vol. 51, n. 4, 2000, 605-622.

Hansell, Saul, « Google Wants to Dominate Madison Avenue, Too », *The New York Times*, 30 octobre 2005, URL : www.nytimes.com/2005/10/30/business/yourmoney/google-wants-to-dominate-madison-avenue-too.html?_r=0 (consulté le 11 mars 2017).

Harcourt, Bernard, *Exposed : Desire and Disobedience in the Digital Age*, Harvard University Press, 2015.

Hardt, Michael et Antonio Negri, *Empire*, Harvard University Press, 2001.

Hargittai, Eszter, *Holes in the Net : The Internet and International Stratification*, 1996, URL : http://www.isoc.org/inet98/proceedings/5d/5d_1.htm (consulté le 4 décembre 2017).

Harvey, David, « The ‘‘New Imperialism’’ : Accumulation by Dispossession », *Actuel Marx*, vol. 1, n. 35, 2004, 71-90.

Hier, Sean, « Probing the Surveillant Assemblage : on the dialectics of surveillance practices as processes of social control », *Surveillance & Society*, vol. 1, n. 3, 2003, 399-411.

Highham, Pam, « Keeping it real : A critique of postmodern theories of cyberspace », chapitre dans Jose Lopez et Garry Potter, *After Postmodernism : An Introduction to Critical Realism*, A&C Black, 2005.

Hopkins, Nick et Julian Borger, « Exclusive : NSA pays £100m in secret funding for GCHQ », *The Guardian*, 1er août 2013, URL : https://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden (consulté le 4 juillet 2017).

Hopkins, Nick, « UK gathering secret intelligence via covert NSA operation », *The Guardian*, 7 juin 2013, URL : https://www.theguardian.com/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism (consulté le 6 juillet 2017).

Hurley, Matthew, « For and From Cyberspace – Conceptualizing Cyber Intelligence, Surveillance, and Reconaissance », *Air & Space Power Journal*, novembre-décembre 2012, 12-33.

Idhe, Don, *Bodies in Technology*, University of Minnesota Press, 2002.

Institute for National Strategic Studies, *Joint Vision 2020. America’s Military – Preparing for Tomorrow*, U.S. Government Printing Office, 2000, 61, URL : http://www.dtic.mil/dtic/tr/fulltext/u2/a526044.pdf (consulté le 17 juillet 2017).

Jablonsky, David, « The State of the National Security State », *The US Army War College*

Quarterly Parameters, vol. 43, n. 4, hiver 2002-2003, 4-20.

Joint Chiefs of Staff, *Cyberspace Operations*, 5 février 2013, II-5, URL : http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf (consulté le 19 août 2017).

Joseph Skovira, Robert, « The Social Contract Revised : Obligation and Responsibility in the Information Society », chapitre dans Hamid Nemati, *Information Security and Ethics : Concepts, Methodologies, Tools, and Applications*, IGI Global, 2007.

Joubert, Vincent, « De l'importance stratégique du cyberespace », *Analyse stratégique*, 9 novembre 2010, URL : https://dandurand.uqam.ca/wp-content/uploads/sites/3/2016/04/Joubert_cyberespace091110.pdf (consulté le 8 juin 2017).

Kalanje, M. Christopher, « Role of Intellectual Property in Innovation and New Product Development », *World Intellectual Property Organization*, s/d, URL : http://www.wipo.int/sme/en/documents/ip_innovation_development_fulltext.html (consulté le 19 août 2017).

Kane, Alex, « How Israel Became a Hub for Surveillance Technology », *The Intercept*, 17 octobre 2016, URL : https://theintercept.com/2016/10/17/how-israel-became-a-hub-for-surveillance-technology/ (consulté le 1er juillet 2017).

Keohane, O. Robert et Joseph S. Nye, « Power and interdependence in the information age », *Foreign Affairs*, vol. 77, n. 5, septembre-octobre 1998, 81-94.

Kerry, John, « Kerry : Some of NSA's 'Actions 'reached Too Far' », *Youtube*, 1 novembre 2013, URL : www.youtube.com/watch?v=hWIdYFog464 (consulté le 21 juillet 2017).

Kerschberg, Ben, « Five Steps to Master Big Data and Predictive Analytics in 2014 », *Forbes*, 2014, URL : www.forbes.com/sites/benkerschberg/2014/01/03/five-steps-to-master-big-data-and-predictive-analytics-in-2014/#2f018a816f43 (consulté le 1 décembre 2017).

Knight, Judson, « Dual Use Technology », section dans K. Lee Lerner et Brenda Lerner, *Encyclopedia of Espionage, Intelligence, and Security*, Gale, 2004.

Kopstein, Joshua, « The NSA Can 'Collect-it-All', But What Will It Do With Our Data Next? », *The Daily Beast*, 16 mai 2014, URL : http://www.thedailybeast.com/articles/2014/05/16/the-nsa-can-collect-it-all-but-what-will-it-do-with-our-data-next.html (consulté le 1 décembre 2017).

Krige, John, *American Hegemony and the Postwar Reconstruction of Science in Europe*, The MIT Press, 2008.

Lanier, Jaron, *Who Owns the Future*, Simon & Schuster, 2014.

Larson, Jeff *et al.*, « A Trail of Evidence Leading to AT&T's Partnership with the NSA », *ProPublica*, 15 août 2015, URL : https://www.propublica.org/article/a-trail-of-evidence-leading-to-atts-partnership-with-the-nsa (consulté le 4 août 2017).

Lascoumes, Pierre, « La Gouvernementalité : de la critique de l'État aux technologies du pouvoir », *Le Portique*, n. 3-4, 2004, URL : http://leportique.revues.org/625#abstract (consulté le 1 décembre 2017).

Lazzarato, Mauricio, *Les révolutions du capitalisme*, Seuil, 2004.

Lee, Micah, Glenn Greenwald et Morgan Marquis-Boire, « XKEYSCORE – NSA's Google for the World's Private Communications », *The Intercept*, 1 juillet 2015, URL : https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications (consulté le 14 juin 2017).

Legal Information Institute, *47 U.S. Code Subchapter I – Interception of Digital and Other Communications*, 2017, URL : https://www.law.cornell.edu/uscode/text/47/chapter-9/subchapter-I (consulté le 22 juin 2017).

Lemke, Thomas, *Foucault, Governmentality, and Critique*, Routledge, 2015.

Levy, Steven, « Exclusive : How Google's Algorithm Rules the Web », *Wired*, 22 février 2010, URL : https://web.archive.org/web/20110612022158/http://www.wired.com/magazine/2010/02/ff_google_algorithm/2 (consulté le 9 mars 2017).

Levy, Steven, « Google Throws Open Doors to Its Top-Secret Data Center », *Wired*, 17 octobre 2012, URL : http://www.wired.com/2012/10/ff-inside-google-data-center/ (consulté le 1 décembre 2017).

Lightfoot, Geoffrey et Tomasz Wisniwski, *Information Asymmetry and Power in a Surveillance Society*, MPRA, 2014, URL : https://mpra.ub.uni-muenchen.de/58726/8/MPRA_paper_58726.pdf (consulté le 2 août 2017).

Lima, Joao, « Top 10 biggest data centres from around the world », *Computer Business Review*, 2 avril 2015, URL : http://www.cbronline.com/news/data-centre/top-10-biggest-data-centres-from-around-the-world-4545356/ (consulté le 9 juin 2017).

Luchetta, Giacomo, *Is The Google Platform a Two-Sided Market ?*, SSRN, 2012, URL : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2048683 (consulté le 6 mars 2017).

Lyon, David, « Cyberspace sociality », chapitre dans Brian Loader, *The Governance of Cyberspace: Politics, Technology and Global Restructuring*, Routledge, 1997.

Lyon, David, « Liquid Surveillance : The Contribution of Zygmunt Bauman to Surveillance Studies », *International Political Sociology*, n. 4, 2010, 325-338.

Lyon, David, « Surveillance, Snowden, and Big Data : Capacities, consequences, critique », *Big Data & Society*, juillet 2014, 1-13.

Lyon, David, « The Politics of Surveillance », chapitre dans *Surveillance Society : Monitoring Everyday Life*, McGraw-Hill Education, 2001.

Lyon, David, *Surveillance Studies : An Overview*, Polity Press, 2007.

Lyotard, Jean-François, *The Postmodern Condition : A Report on Knowledge*, University of Minnesota Press, 1984.

MacAskill, Ewen et Gabriel Dance, « NSA Files : Decoded – What the revelations mean for you », *The Guardian*, 1 novembre 2013, URL : https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1 (consulté le 10 juin 2017).

MacAskill, Ewen, « NSA paid millions to cover Prism compliance costs for tech companies », *The Guardian*, 23 août 2013, URL : https://www.theguardian.com/world/2013/aug/23/nsa-prism-costs-tech-companies-paid (consulté le 6 juillet 2017).

MacAskill, Ewen, « The NSA's bulk metadata collection authority just expired. What now? », *The Guardian*, 28 novembre 2015, URL : https://www.theguardian.com/us-news/2015/nov/28/nsa-bulk-metadata-collection-expires-usa-freedom-act (consulté le 11 juin 2017).

MacAskill, Ewen, Julian Borger, Nick Hopkins *et al.*, « GCHQ taps fibre-optic cables for secret access to world's communications », *The Guardian*, 21 juin 2013, URL : https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa (consulté le 12 juin 2017).

MacGregor, D. et al., « Convergence Platforms : Human-Scale Convergence and the Quality of Life », chapitre dans Milhail Roco et al., *Convergence of Knowledge, Technology and Society : Beyond Convergence of Nano-Bio-Info-Cognitive Technologies*, Springer Science & Business Media, 2014.

Madrigal, Alexis, « The World Is Not Enough : Google and the Future of Augmented Reality », *The Atlantic*, 25 octobre 2012, URL

https://www.theatlantic.com/technology/archive/2012/10/the-world-is-not-enough-google-and-the-future-of-augmented-reality/264059/ (consulté le 11 mars 2017).

Magalhaes, Roy, *Organizational Knowledge and Technology : An Action-Oriented Perspective on Organization and Information Systems*, Edward Elgar Publishing, 2004.

Malik, Mohan, « Technopolitics : How Technology Shapes Relations Among Nations », chapitre dans Watson, Virgina Bacay. *The Interface of Science, Technology & Security : Areas of Most Concern, Now and Ahead*, Asia-Pacific Center for Security Studies, 2012.

Mann, Steve, Jason Nolan et Barry Wellman, « Sousveillance : Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments », *Surveillance & Society*, vol. 1, n. 3, 2003, 332-355.

Marx, Gary, « What's New About the ''New Surveillance''? Classifying for Change and Continuity », *Surveillance & Society*, vol. 1, n. 1, 9-29.

Mayer-Schoenberger, V. et K. Cukier, *Big Data – A Revolution that will transform how we live, work, and think*, John Murray Publishers, 2013.

McEvoy Manjikian, Mary, « From Global Village to Virtual Battlespace : The Colonizing of the Internet and the Extension of Realpolitik », *International Studies Quarterly*, vol. 54, n. 2, 2010, 381-401.

McLuhan, Marshall et Quentin Fiore, *The Medium is the Massage - An Inventory of Effects*, Gingko Pr Inc, 2001.

McRae, Hamish, « Facebook, Airbnb, Uber, and the unstoppable rise of the content non-generators », *The Independent*, 5 mai 2015, URL http://www.independent.co.uk/news/business/comment/hamish-mcrae/facebook-airbnb-uber-and-the-unstoppable-rise-of-the-content-non-generators-10227207.html (consulté le 8 mars 2017).

McStay, Andrew, *Digital Advertising*, Palgrave Macmillan, 2009.

Miller, David, « Information Dominance : The Philosophy of Total Propaganda Control? », chapitre dans Yahya Kamalipour et Nancy Snow, *War, Media and Propaganda : A Global Perspective*, Rowman & Littlefield Publishers, 2004.

Mody, Arjun et Corinne Curcie, *The New Imperial Presidency*, Harvard Political Review, 7 décembre 2011, URL : http://harvardpolitics.com/covers/constitution/the-new-imperial-presidency/ (consulté le 2 août 2017).

Morin, Edgar, *Introduction à la pensée complexe*, Éditions du Seuil, 2005.

Mort, Sébastien, « Surveillance des correspondances privées dans le cyberespace aux États-Unis », *Revue française d'études américaines*, vol. 1, n. 123, 2010, 33-53.

Mowshowitz, Abbe, *Virtual Organization : Toward a Theory of Societal Transformation Stimulated by Information Technology*, Greenwood Publishing Group, 2002.

Mulligan, Thomas, « The Internet Backbone », *Los Angeles Times*, 3 février 1997, URL : http://articles.latimes.com/1997-02-03/business/fi-25071_1_internet-backbone (consulté le 1er juillet 2017).

Murakami Wood, David, « Editorial : Foucault and Panopticism Revisited », *Surveillance & Society*, vol. 1, n. 3, 234-239.

Murakami Wood, David, « Vanishing Surveillance : Why Seeing What is Watching Us Matters », *Office of the Privacy Commissioner of Canada*, 2011, URL www.priv.gc.ca/information/research-recherche/2011/wood_201107_e.asp (consulté le 1 décembre 2017).

Nakashima, Ellen et Joby Warrick, « For NSA chief, terrorist threat drives passion to 'collect it all' », *The Washington Post*, 14 juillet 2013, URL https://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html (consulté le 4 décembre 2017).

Napier Tye, John, « Meet Executive order 12333 : The Reagan rule that lets the NSA spy on Americans », *The Washington Post*, 18 juillet 2014, URL : https://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html?utm_term=.e6f5e71d4aee (consulté le 28 juin 2017).

Narayana, Nagesh, « Google, Facebook and Youtube outshine others in web globalization », *International Business Times*, 2011, URL http://www.ibtimes.com/google-facebook-youtube-outshine-others-web-globalization-278813 (consulté le 1 décembre 2017).

National Research Council, *Persistent Forecasting of Disruptive Technologies*, The National Academies Press, 2010.

National Security Agency, « Newly Disclosed N.S.A. Files Detail Partnerships With AT&T and Verizon », *The New York Times*, 15 août 2015, URL : https://www.nytimes.com/interactive/2015/08/15/us/documents.html (consulté le 29 juin 2017).

National Security Agency, *Customers & Partners*, 27 mai 2016, URL :

https://www.nsa.gov/what-we-do/customers-and-partners/ (consulté le 7 juillet 2017).

National Security Agency, *Cyber*, 19 juillet 2017, URL : https://www.nsa.gov/what-we-do/cyber/ (consulté le 19 juillet 2017).

National Security Agency, *Statement – NSA Stops Certain Section 702 ''Upstream'' Activities*, 28 avril 2017, URL : https://www.nsa.gov/news-features/press-room/statements/2017-04-28-702-statement.shtml (consulté le 3 juillet 2017).

National Security Agency, *Understanding the Threat*, 3 mai 2016, URL : https://www.nsa.gov/what-we-do/understanding-the-threat/ (consulté le 9 juillet 2017).

Neil Cukier, Kenneth et Viktor Mayer-Schoenberger, « The Rise of Big Data – How It's Changing the Way We Think About the World », *Foreign Affairs*, mai-juin 2013, URL https://www.foreignaffairs.com/articles/2013-04-03/rise-big-data (consulté le 1 décembre 2017).

Noam, Eli, *The Effect of Deregulation on Market Concentration : an Analysis of the Telecom Act of 1996 and the Industry Meltdown*, 2002, URL www.citi.columbia.edu/elinoam/articles/Effect_of_Deregulation_on_MarketConcentration.pdf (consulté le 1 décembre 2017).

Nye, S. Joseph, « The Information Revolution and American Soft Power », *Asia-Pacific Review*, vol. 9, n. 1, 2002, 60-76.

O'Harrow Jr., Robert et Ellen Nakashima, « President's Surveillance Program worked with private sector to collect data after Sept. 11, 2001 », *The Washington Post*, 27 juin 2013, URL : https://www.washingtonpost.com/investigations/presidents-surveillance-program-worked-with-private-sector-to-collect-data-after-sept-11-2001/2013/06/27/2c7a7e74-df57-11e2-b2d4-ea6d8f477a01_story.html?utm_term=.3e03479c1581 (consulté le 26 juin 2017).

O'Neill, John, « Bio-Technology : Empire, Communications and Bio-Power », *Canadian Journal of Political and Social Theory*, vol. 10, n. 1-2, 1986, 68-78.

Office of the Director of National Intelligence, « Fact Sheet on E.O. 12333 Raw SIGINT Availability Procedures », *IC on the Record*, 12 janvier 2017, URL : https://www.dni.gov/files/documents/icotr/FactSheetEO12333RawSIGINTProcedures.pdf (consulté le 28 juin 2017).

Oxford University Press, *Surveillance*, 2016, URL http://www.oxforddictionaries.com/definition/english/surveillance (consulté le 1 décembre 2017).

Palier, Bruno, « *Path dependence* (Dépendance au chemin emprunté) », section dans Boussaquet, Laurie *et al.*, *Dictionnaire des politiques publiques*, Presses de Sciences Po, 2010.

Paul Marshall, Jonathan, *Living on Cybermind: Categories, Communication, and Control*, Peter Lang, 2007.

PBS, « Spying on the Home Front : Interview – Mark Klein », *Frontline*, 15 mai 2007, URL : http://www.pbs.org/wgbh/pages/frontline/homefront/interviews/klein.html (consulté le 1er juillet 2017).

Perez, Evan, « Secret Court's Oversight Gets Scrutiny », *The Wall Street Journal*, 9 juin 2013, URL : https://www.wsj.com/articles/SB10001424127887324904004578535670310514616 (consulté le 17 août 2017).

Perry Barlow, John, « A Declaration of the Independence of Cyberspace », *Electronic Frontier Foundation*, 1996, URL www.eff.org/cyberspace-independence (consulté le 1 décembre 2017).

Piero Siroli, Gian, « Strategic Information Warfare : An Introduction », chapitre dans Martin Bayer, *Cyberwar, Netwar and the Revolution in Military Affairs*, Palgrave MacMillan, 2006.

Post, David, « Governing Cyberspace », *The Wayne Law Review*, vol. 43, n. 1, 1996, 883-913.

Powell, A., « 'Datafication', Transparency, and Good Governance of the Data City », chapitre dans K. O'Hara, M-H. C. Nguyen et P. Haynes, *Digital Enlightenment Yearbook 2014 : Social Networks and Social Machines, Surveillance and Empowerment*, IOS Press, 2014.

Price, E. Monroe, *Media and Sovereignty – The Global Information Revolution and Its Challenge to State Power*, The MIT Press, 2002.

Priest, Dana, « NSA growth fueled by need to target terrorists », *The Guardian*, 21 juillet 2013, URL : https://www.washingtonpost.com/world/national-security/nsa-growth-fueled-by-need-to-target-terrorists/2013/07/21/24c93cf4-f0b1-11e2-bed3-b9b6fe264871_story.html?utm_term=.7c3f62b09f83 (consulté le 13 juillet 2017).

Purkayastha, P., « New Technologies and Emerging Structures of Global Dominance », *Economic and Political Weekly*, vol. 29, n. 35, 1994, 102-108.

Ralston, Joseph et Paul Kaminiski, « Chapter IV – Achieving Joint Warfighting Capability Objectives : Information Superiority », *Joint Warfighter S&T Plan*, 1997, URL http://fas.org/spp/military/docops/defense/97_jwstp/jw4a.htm (consulté le 1 décembre 2017).

Rappert, Brian, *Technology and Security : Governing Threats in the New Millenium*, Springer, 2007.

Reidenberg, Joel et Thomas Davenport, « Should the U.S. Adopt European-Style Data-Privacy Protections ? », *The Wall Street Journal*, 10 mars 2013, URL https://www.wsj.com/articles/SB10001424127887324338604578328393797127094 (consulté le 14 mars 2017).

Reynaud, Florian, « Le business des ‘‘zero day’’, ces failles inconnues des fabricants de logiciel », *Le Monde*, 23 septembre 2015, URL : http://www.lemonde.fr/pixels/article/2015/09/23/le-business-des-zero-day-ces-failles-inconnues-des-fabricants-de-logiciel_4768638_4408996.html (consulté le 1 août 2017).

Richard, Claire, « Surveiller, tout en se cachant, est la forme la plus haute du pouvoir », *L'Obs*, 26 août 2016, URL : http://tempsreel.nouvelobs.com/rue89/rue89-le-grand-entretien/20160826.RUE7798/surveiller-tout-en-se-cachant-est-la-forme-la-plus-haute-du-pouvoir.html#link_time=1472220110 (consulté le 28 octobre 2017).

Risen, James et Eric Lichtblau, « Bush Lets U.S. Spy on Callers Without Courts », *The New York Times*, 16 décembre 2005, URL : http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html (consulté le 27 juin 2017).

Rose, Nikolas et Peter Miller, « Political Power Beyond the State: Problematics of Government », *The British Journal of Sociology*, vol. 43, n. 2, 1992, 172-205.

Rosenberg, Eric, « The Business of Google (GOOG) », *Investopedia*, 5 août 2016, URL http://www.investopedia.com/articles/investing/020515/business-google.asp (consulté le 11 mars 2017).

Ruffolo, V. David, « Rhizomatic Bodies : Thinking through the Virtualities of Control Societies », *Rhizomes*, n. 17, 2008, URL www.rhizomes.net/issue17/ruffolo.html (consulté le 1 décembre 2017).

Russia Today, *'Country X' : WikiLeaks reveals NSA recording 'nearly all' phone calls in Afghanistan*, 24 mai 2014, URL : https://www.rt.com/news/160988-wikileaks-nsa-phone-afghanistan/ (consulté le 5 juillet 2017).

Samaan, Jean-Loup, « Mythes et réalités des cyberguerres », *Politique étrangère*, n. 4, hiver 2008, 829-841.

Schmidt, Eric et Jared Cohen, « The Digital Disruption : Connectivity and the Diffusion of Power », *Foreign Affairs*, vol. 89, n. 6, 2010, URL :

https://www.foreignaffairs.com/articles/2010-10-16/digital-disruption (consulté le 4 décembre 2017).

Schneier, Bruce, « 'Stalker Economy' here to stay », *CNN*, 26 novembre 2013, URL http://edition.cnn.com/2013/11/20/opinion/schneier-stalker-economy/index.html (consulté le 1 décembre 2017).

Schneier, Bruce, *Data & Goliath – The Hidden Battles to Collect Your Data and Control Your World*, W. W. Norton & Company, 2015.

Schumpeter, A. Joseph, *Capitalism, Socialism and Democracy*, Harper, 1942.

Scott, C. James, *Seeing Like A State : How Certain Schemes to Improve the Human Condition Have Failed*, Yale University Press, 1999.

Scott, David, « Colonial Governmentality », *Social Text*, n. 43, 1995, 191-220.

Simon, Bart, « The Return of Panopticism : Supervision, Subjection and the New Surveillance », *Surveillance & Society*, vol. 3, n. 1, 1-20.

Singer, P. W. et Allan Friedman, *Cybersecurity and Cyberwar – What everyone needs to know*, Oxford University Press, 2014.

Sneed, Annie, « Moore's Law Keeps Going, Defying Expectations », *Scientific American*, 2015, URL : http://www.scientificamerican.com/article/moore-s-law-keeps-going-defying-expectations/ (consulté le 4 décembre 2017).

Sottek, T.C. et Janus Kopfstein, « Everything you need to know about PRISM », *The Verge*, 17 juillet 2013, URL : https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet (consulté le 5 juillet 2017).

Spiegel Staff, « Inside TAO : Documents Reveal Top NSA Hacking Unit – Part 3 : The NSA's Shadow Network », *Spiegel Online*, 29 décembre 2013, URL : http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969-3.html (consulté le 1 août 2017).

Stuart, T. Douglas, *Creating the National Security State: A History of the Law that Transformed America*, Princeton University Press, 2009.

Surveillance & Society, *Journal History*, 2016, URL : http://library.queensu.ca/ojs/index.php/surveillance-and-society/about/history (consulté le 1 décembre 2017).

Surveillance Studies Centre, *About*, 2016, URL : www.sscqueens.org/about (consulté le 1 décembre 2017).

Taylor, Linnet, « Data subjects or data citizens : Adressing the global regulatory challenge of big data », chapitre dans Mireille Hildebrandt, Bibi van den Berg, *Information, Freedom and Property : The Philosophy of Law Meets the Philosophy of Technology*, Routledge, 2016.

Tene, Omer, « What Google Knows : Privacy and Internet Search Engines », *Utah Law Review*, 2008, 1433-1492.

The Economist, « Should digital monopolies be broken up ? », *The Economist*, 29 novembre 2014, URL http://www.economist.com/news/leaders/21635000-european-moves-against-google-are-about-protecting-companies-not-consumers-should-digital (consulté le 1 décembre 2017).

The Economist. *The Right to be left alone*, 19 janvier 2015, URL www.economist.com/news/science-and-technology/21639988-why-do-people-cherish-privacy-yet-cheerfully-surrender-it-right-be-left-alone (consulté le 1 décembre 2017).

The Guardian, « Google dominates search. But the real problem is its monopoly on data », 19 avril 2015, URL https://www.theguardian.com/technology/2015/apr/19/google-dominates-search-real-problem-monopoly-data (consulté le 15 avril 2017).

The Guardian, *NSA Prism program slides*, 1 novembre 2013, 4, URL : https://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document (consulté le 3 août 2017).

The Intercept. *Elegant Chaos : collect it all, exploit it all (plus notes)*, 6 septembre 2016, URL : https://theintercept.com/document/2016/09/06/elegant-chaos-collect-it-all-exploit-it-all-plus-notes/ (consulté le 23 octobre 2017).

Thompson, Derek, « Google's CEO : 'The Laws Are Written by Lobbyists' », *The Atlantic*, 1 octobre 2010, URL www.theatlantic.com/technology/archive/2010/10/googles-ceo-the-laws-are-written-by-lobbyists/63908/ (consulté le 4 mars 2017).

Tillinac, Jean, « Le web 2.0 ou l'avènement du client ouvrier », *Quaderni*, vol. 60, n. 1, 2006, 19-24.

Timberg, Craig, « NSA slide shows surveillance of undersea cables », *The Washington Post*, 10 juillet 2013, URL : https://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html?utm_term=.77d0cac92628 (consulté le 3 juillet 2017).

U.S. Department of Defense, *Strategy for Operations in the Information Environment*, juin 2016, URL : https://www.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf (consulté le 11 juillet 2017).

U.S. Department of Justice, « Justice Department and NSA memos proposing broader powers for NSA to collect data », *The Guardian*, 27 juin 2013, URL : https://www.theguardian.com/world/interactive/2013/jun/27/nsa-data-collection-justice-department (consulté le 11 juin 2017).

U.S. Department of Justice, *Title III of The Omnibus Crime Control and Safe Streets Act of 1968 (Wiretap Act)*, 19 septembre 2013, URL : https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1284 (consulté le 15 juin 2017).

U.S. Department of State, *National Security Act of 1947*, 2016, URL https://history.state.gov/milestones/1945-1952/national-security-act (consulté le 4 décembre 2017).

United States District Court, « Governement Defendants' Notice of Motion to Dismiss and For Summary Judgment and Memorandum », *Jewel et al. v. National Security Agency et al.*, cas n. 08-cv-4373-VRW, 25 juin 2009, URL : https://www.unitedstatescourts.org/federal/cand/207206/21-0.html (consulté le 4 décembre 2017).

Van Dijck, José, « Datafication, Dataism and Dataveillance : Big Data between scientific paradigm and ideology », *Surveillance & Society*, vol. 2, n. 12, 2014, 197-208.

Varet, Gilbert, *Pour une science de l'information comme discipline rigoureuse*, Paris, Les Belles Lettres, 1987.

Verde Garrido, Miguelangel, « Contesting a Biopolitics of Information and Communication », *Surveillance & Society*, vol. 13, n. 2, 2015, 153-167.

Watkins, Ali, « Most of NSA's data collection authorized by order Ronald Reagan issued », *McClatchy Washington Bureau*, 21 novembre 2013, URL : http://www.mcclatchydc.com/news/nation-world/national/national-security/article24759289.html (consulté le 29 juin 2017).

Watts, Jonathan, « NSA accused of spying on Brazilian oil company Petrobras », *The Guardian*, 9 septembre 2013, URL : https://www.theguardian.com/world/2013/sep/09/nsa-spying-brazil-oil-petrobras (consulté le 12 juillet 2018).

Wiedner, Jason, « Governmentality, Capitalism and Subjectivity », *Global Society*, vol. 23, n. 4, octobre 2009, 387-411.

Winner, Langdon, *Autonomous Technology : Technics-out-of-Control as a Theme in Political Thought*, The MIT Press, 1978.

Wired Staff, « AT&T Whistle-blower's evidence », *Wired*, 17 mai 2006, URL : https://www.wired.com/2006/05/att-whistle-blowers-evidence/ (consulté le 1er juillet 2017).

Yuhas, Alan, « NSA reform : USA Freedom Act passes first surveillance reform in decade – as it happened », *The Guardian*, 2 juin 2015, URL : https://www.theguardian.com/us-news/live/2015/jun/02/senate-nsa-surveillance-usa-freedom-act-congress-live?page=with:block-556e1ba8e4b07871543bacf5#block-556e1ba8e4b07871543bacf5 (consulté le 29 juillet 2017).

Yusuf, Muhammad et Carl Adams, « A Base of Knowledge, Mobile, and Web 2.0 Technologies for Connected E-Government », chapitre dans Mahmood Zaigham, *Emerging Mobile and Web 2.0 Technologies for Connected E-Government*, IGI Global, 2014.

Zavala Pérez, Maria, « Registry Culture and Networked Sociability : Building Individual Identity through Information Records », chapitre dans Francesca Comunello, *Networked Sociability and Individualism : Technology for Personal and Professional Relationships*, IGI Global, 2011.